

# William & Mary Bill of Rights Journal

---

Volume *Volume 22 (2013-2014)*  
Issue 2 *Professor Charles H. Koch, Jr. Memorial*  
*Symposium on Administrative Law*

---

Article 14

December 2013

## Administrative Searches, Technology and Personal Privacy

Russell L. Weaver

Follow this and additional works at: <https://scholarship.law.wm.edu/wmborj>



Part of the [Administrative Law Commons](#), and the [Fourth Amendment Commons](#)

---

### Repository Citation

Russell L. Weaver, *Administrative Searches, Technology and Personal Privacy*, 22 Wm. & Mary Bill Rts. J. 571 (2013), <https://scholarship.law.wm.edu/wmborj/vol22/iss2/14>

Copyright c 2013 by the authors. This article is brought to you by the William & Mary Law School Scholarship Repository.

<https://scholarship.law.wm.edu/wmborj>

## ADMINISTRATIVE SEARCHES, TECHNOLOGY AND PERSONAL PRIVACY

Russell L. Weaver\*

Although administrative searches have been conducted since the British colonial period, modern administrative searches have become potentially more intrusive because of advances in technology. Agencies still conduct many of the same types of searches that they have historically conducted. For example, federal administrative officials screen airline passengers,<sup>1</sup> and search liquor stores,<sup>2</sup> firearms and ammunition dealers,<sup>3</sup> pharmacies,<sup>4</sup> employee work sites,<sup>5</sup> mines,<sup>6</sup> the nation's borders,<sup>7</sup> schools,<sup>8</sup> and prisons.<sup>9</sup> In addition, state and local officials inspect restaurants (for health and sanitation reasons),<sup>10</sup> auto junkyards,<sup>11</sup> and the homes of welfare recipients.<sup>12</sup> However, in recent years, new questions have arisen regarding whether administrative inspectors can examine the contents of electronic devices such as laptops and iPhones.

The U.S. Supreme Court's administrative-search jurisprudence has been chaotic at best.<sup>13</sup> At times, the Court has expressed doubt about whether the Fourth Amendment

---

\* Professor of Law & Distinguished University Scholar, University of Louisville, Louis D. Brandeis School of Law.

<sup>1</sup> See *About TSA*, TSA, <http://www.tsa.gov/about-tsa> (last visited Dec. 12, 2013).

<sup>2</sup> See *Colonnade Catering Corp. v. United States*, 397 U.S. 72, 73–74 (1970).

<sup>3</sup> See *Firearms Enforcement*, U.S. DEP'T OF JUSTICE, BUREAU OF ALCOHOL, TOBACCO, FIREARMS & EXPLOSIVES, <http://www.atf.gov/content/Firearms/firearms-enforcement> (last visited Dec. 12, 2013); see also *United States v. Biswell*, 406 U.S. 311, 311–12 (1972).

<sup>4</sup> See *Inspectional Authority; Refusal to Permit Inspection*, U.S. FDA, <http://www.fda.gov/ICECI/ComplianceManuals/CompliancePolicyGuidanceManual/ucm073839.htm> (last visited Dec. 12, 2013).

<sup>5</sup> See U.S. DEP'T OF LABOR, OSHA, <http://www.osha.gov/dep/index.html> (last visited Dec. 12, 2013); see also *Marshall v. Barlow's, Inc.*, 436 U.S. 307, 309 (1978).

<sup>6</sup> See *About FMSHRC*, FED. MINE SAFETY & HEALTH REVIEW COMM'N, <http://www.fmshrc.gov/about> (last visited Dec. 12, 2013); see also *Donovan v. Dewey*, 452 U.S. 594, 596 (1981).

<sup>7</sup> See *United States v. Flores-Montano*, 541 U.S. 149, 152–53 (2004); *United States v. Ramsey*, 431 U.S. 606, 611–12 (1977).

<sup>8</sup> See *New Jersey v. T.L.O.*, 469 U.S. 325, 340 (1985).

<sup>9</sup> See *Hudson v. Palmer*, 468 U.S. 517, 525–26 (1984).

<sup>10</sup> See *Camuglia v. City of Albuquerque*, 448 F.3d 1214, 1220–21 (10th Cir. 2006).

<sup>11</sup> See *New York v. Burger*, 482 U.S. 691, 707 (1987).

<sup>12</sup> See *Wyman v. James*, 400 U.S. 309, 326 (1971).

<sup>13</sup> See *infra* notes 14–22 and accompanying text. The Fourth Amendment reads:

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.

should apply to administrative inspections at all. For example, in *Frank v. Maryland*,<sup>14</sup> the Court flatly stated that some administrative inspections, such as municipal fire, health, and housing inspection programs, “touch at most upon the periphery of the important interests safeguarded by the Fourteenth Amendment’s protection against official intrusion.”<sup>15</sup> In *Frank*, the Court was willing to permit administrative inspections because it concluded that they were accompanied by a long history of public acceptance.<sup>16</sup> Although *Camara v. Municipal Court*<sup>17</sup> eventually made it clear that the Fourth Amendment applies to administrative inspections,<sup>18</sup> the Court’s administrative-search decisions have always treated such inspections as an anomaly in the Court’s Fourth Amendment jurisprudence.<sup>19</sup> In particular, the Court has suggested that administrative searches are fundamentally different than police searches for evidence of “traditional” crimes such as robbery, rape, murder, or burglary,<sup>20</sup> and the Court has imposed different and lesser requirements for administrative searches.<sup>21</sup> In addition, the Court has upheld warrantless administrative searches in various contexts.<sup>22</sup>

In a modern society, the Court’s failure to develop a coherent approach to administrative inspections creates troubling implications for personal privacy. The difficulty is illustrated by the so-called border-search exception to the warrant requirement, which allows customs and immigration officials broad authority to conduct searches at the U.S. border.<sup>23</sup> Concerns regarding the privacy implications of this exception were first raised by Professors Janet C. Hoeffel and Stephen Singer.<sup>24</sup> Every day, thousands of people enter the United States from other countries.<sup>25</sup> In a modern society, driven by technological innovation, these individuals often carry electronic devices such as laptops, electronic readers, smart phones, and iPads. Not only can these electronic devices store large amounts of information, they can connect to servers and clouds where

---

U.S. CONST. amend. IV. The Fourth Amendment’s protections have been incorporated into the Fourteenth Amendment, and therefore are applicable to the states. *See Camara v. Mun. Court*, 387 U.S. 523, 528 (1967); *Ker v. California*, 374 U.S. 23, 30 (1963).

<sup>14</sup> 359 U.S. 360 (1959), *overruled by* *Camara v. Mun. Court*, 387 U.S. 523 (1967).

<sup>15</sup> *Id.* at 367.

<sup>16</sup> *Id.* at 364–68.

<sup>17</sup> 387 U.S. 523 (1967).

<sup>18</sup> *Id.* at 528, 530–31.

<sup>19</sup> *See, e.g., Boyd v. United States*, 116 U.S. 616, 623–24 (1886).

<sup>20</sup> *See, e.g., Frank*, 359 U.S. at 365–66.

<sup>21</sup> *Id.* at 372.

<sup>22</sup> *See Camara*, 387 U.S. at 539; *N. Am. Cold Storage Co. v. City of Chicago*, 211 U.S. 306, 315–16 (1908); *Jacobson v. Massachusetts*, 197 U.S. 11, 37–38 (1905); *Compagnie Francaise de Navigation a Vapeur v. La. State Bd. of Health*, 186 U.S. 380, 387 (1902).

<sup>23</sup> *See United States v. Flores-Montano*, 541 U.S. 149, 152–53 (2004); *United States v. Ramsey*, 431 U.S. 606, 616 (1977).

<sup>24</sup> *See Janet C. Hoeffel & Stephen Singer, Fear and Loathing at the U.S. Border*, 82 *MISS. L.J.* 833 (2013).

<sup>25</sup> *See id.* at 840 n.35.

additional information is stored.<sup>26</sup> Historically, the U.S. government has exercised broad authority to search individuals at the border, including their luggage, papers, and effects.<sup>27</sup> In an era of technological innovation, questions have arisen regarding whether customs officials can review all information stored on electronic devices being carried across the U.S. border and whether they can retain those electronic devices, or copy the information stored on them.<sup>28</sup> The U.S. Department of Homeland Security (DHS) takes the position that it has broad authority to search, retain, or copy electronic information.<sup>29</sup>

This Article offers a glimpse at the historical underpinnings of the Fourth Amendment, especially in the administrative context and suggests that administrative searches have historically been treated as stepchildren in the Court's Fourth Amendment jurisprudence. The U.S. Supreme Court has been more willing to sustain governmental actions in the administrative context than it has been willing to sustain in other contexts. The Article goes on to conclude that, in a modern world that is driven by technological innovation, the Court's approach to administrative searches, and in particular to border searches, threatens to significantly undermine personal privacy.

#### I. ADMINISTRATIVE SEARCHES IN THE FOURTH AMENDMENT CONTEXT

When the history of the Fourth Amendment is analyzed, it is not clear that there is a clear dividing line between administrative searches and "other" types of searches. Many of the abuses during the colonial period—abuses that led the new Americans to demand protections like those ultimately contained in the Fourth Amendment—involved searches of an administrative nature.<sup>30</sup> One of the practices that particularly

---

<sup>26</sup> *Id.* at 843–44 n.52.

<sup>27</sup> *See Flores-Montano*, 541 U.S. at 152–53; *Ramsey*, 431 U.S. at 616.

<sup>28</sup> *See* Hoeffel & Singer, *supra* note 24, at 833–36.

<sup>29</sup> *See* U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE BORDER SEARCHES OF ELECTRONIC DEVICES 6–8 (2009) [hereinafter *HOMELAND SECURITY ASSESSMENT*], available at [http://www.dhs.gov/xlibrary/assets/privacy/privacy\\_pia\\_cbp\\_laptop.pdf](http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_laptop.pdf).

<sup>30</sup> *See* *Maryland v. Garrison*, 480 U.S. 79, 90 (1987) (Blackmun, J., dissenting) (“The Fourth Amendment, in fact, was a direct response to the colonists’ objection to searches of homes under general warrants or without warrants.”); RUSSELL L. WEAVER ET AL., *PRINCIPLES OF CRIMINAL PROCEDURE* 64–65 (3d ed. 2008) [hereinafter *WEAVER ET AL.* (3d ed.)] (“The debate (and the anger) in the American colonies about the arbitrary use of these writs of assistance by the English ‘was perhaps the most prominent event which inaugurated the resistance of the colonies to the oppressions of the mother country,’” and “[was] fresh in the memories of those who achieved our independence and established our form of government.” (quoting *Boyd v. United States*, 116 U.S. 616, 625 (1886))); *see also* *United States v. Verdugo-Urquidez*, 494 U.S. 259, 266 (1990) (“The driving force behind the adoption of the [Fourth] Amendment . . . was widespread hostility among the former Colonists to the issuance of writs of assistance . . . [T]he purpose of the Fourth Amendment was to protect the people of the United States against arbitrary action by their own Government . . .”).

riled the colonists was the fact that colonial officials could obtain “writs of assistance,” which allowed them to do no more than specify the object of a search and thereby gain authority to search any place where contraband might be found,<sup>31</sup> without limit as to place or duration.<sup>32</sup> Another reviled practice involved the use of “general warrants” that required colonial officials only to specify an offense and then left it to the discretion of executing officials to decide which persons should be arrested and which places should be searched.<sup>33</sup>

During the colonial period, general warrants and writs of assistance were frequently used in the administrative context, particularly in searches conducted by customs officials.<sup>34</sup> As the U.S. Supreme Court recognized in *United States v. Chadwick*,<sup>35</sup> “the Fourth Amendment’s commands grew in large measure out of the colonists’ experience with the writs of assistance,” which “granted sweeping power to customs officials and other agents of the King to search at large for smuggled goods.”<sup>36</sup> Many of these searches involved searches of premises and products to determine whether individuals had complied with revenue laws.<sup>37</sup> Businesses, subjected to the general warrants,

---

<sup>31</sup> See *Virginia v. Moore*, 553 U.S. 164, 168–69 (2008) (“The immediate object of the Fourth Amendment was to prohibit the general warrants and writs of assistance that English judges had employed against the colonists . . . .”); *Samson v. California*, 547 U.S. 843, 858 (2006) (“The pre-Revolutionary ‘writs of assistance,’ which permitted roving searches for contraband, were reviled precisely because they ‘placed ‘the liberty of every man in the hands of every petty officer.’”); *Atwater v. City of Lago Vista*, 532 U.S. 318, 339–40 (2001); see also *WEAVER ET AL.* (3d ed.), *supra* note 30, at 64.

<sup>32</sup> See *Steagald v. United States*, 451 U.S. 204, 220 (1981) (“[T]he writs of assistance used in the Colonies noted only the object of the search—any uncustomed goods—and thus left customs officials completely free to search any place where they believed such goods might be.”); *Gilbert v. California*, 388 U.S. 263, 286 (1967) (“The practice had obtained in the colonies of issuing writs of assistance to the revenue officers empowering them, in their discretion, to search suspected places for smuggled goods, which James Otis pronounced ‘the worst instrument of arbitrary power, the most destructive of English liberty and the fundamental principles of law, that ever was found in an English law book;’ since they placed ‘the liberty of every man in the hands of every petty officer.’” (quoting *Boyd*, 116 U.S. at 625)).

<sup>33</sup> See *Moore*, 553 U.S. at 168–69; *Steagald*, 451 U.S. at 220; *Payton v. New York*, 445 U.S. 573, 608 (1980) (White, J., dissenting) (“[I]t was the abusive use of the warrant power, rather than any excessive zeal in the discharge of peace officers’ inherent authority, that precipitated the Fourth Amendment. That Amendment grew out of colonial opposition to the infamous general warrants known as writs of assistance, which empowered customs officers to search at will, and to break open receptacles or packages, wherever they suspected uncustomed goods to be.”).

<sup>34</sup> See *Payton*, 445 U.S. at 583 n.21 (majority opinion).

<sup>35</sup> 433 U.S. 1 (1977).

<sup>36</sup> *Id.* at 7–8.

<sup>37</sup> *Marshall v. Barlow’s, Inc.*, 436 U.S. 307, 311 (1978) (“The particular offensiveness it engendered was acutely felt by the merchants and businessmen whose premises and products were inspected for compliance with the several parliamentary revenue measures that most irritated the colonists.”).

objected vociferously to these inspections.<sup>38</sup> In *Frank*,<sup>39</sup> even though the Court concluded that administrative searches stand on the periphery of the Fourth Amendment,<sup>40</sup> the Court recognized the importance of administrative inspections to the Fourth Amendment's history and passage.<sup>41</sup> Nevertheless, the Court concluded that administrative searches should receive less protection because Maryland had long permitted administrative inspections without a warrant.<sup>42</sup>

Despite the historical record, the U.S. Supreme Court has given less protection to businesses and individuals in the administrative context.<sup>43</sup> Unquestionably, in a few cases, the Court has recognized that the Fourth Amendment provides special protection to businesses.<sup>44</sup> As the Court stated in *Marshall v. Barlow's, Inc.*, "it is untenable that the ban on warrantless searches was not intended to shield places of business as well as of residence,"<sup>45</sup> and therefore *Marshall* concluded that Fourth Amendment protections should be extended to commercial premises.<sup>46</sup> Nevertheless, the Court's general approach has been to provide fewer protections in the administrative context.

#### A. The Redefinition of Probable Cause

The Court's attitude towards administrative searches is reflected in its definition of "probable cause," and its application of the "particularity" requirement, in the administrative context. For searches conducted outside the administrative context, the Court

---

<sup>38</sup> *Id.* The acts included the Stamp Act of 1765, the Townshend Revenue Act of 1767, and the Tea Tax of 1773. *Id.* at 311 n.7; see *Maryland v. Garrison*, 480 U.S. 79, 90 (1987); *Boyd v. United States*, 116 U.S. 616, 625 (1886); see also *United States v. Verdugo-Urquidez*, 494 U.S. 259, 266 (1990).

<sup>39</sup> 359 U.S. 360 (1959).

<sup>40</sup> *Id.* at 367.

<sup>41</sup> *Id.* at 363. The Court noted that the history of the constitutional protection against official invasion of the citizen's home makes explicit the human concerns which it was meant to respect. In years prior to the Revolution leading voiced in England and the Colonies protested against the ransacking by Crown officers of the homes of citizens in search of evidence of crime or of illegally imported goods. The vivid memory by the newly independent Americans of these abuses produced the Fourth Amendment as a safeguard against such arbitrary official action by officers of the new Union, as like provisions had already found their way into State Constitutions.

*Id.*

<sup>42</sup> *Id.* at 373.

<sup>43</sup> See *id.* at 367. The Court in *Frank* acknowledged that "for more than 200 years Maryland has empowered its officers to enter upon ships, carriages, shops, and homes in the service of the common welfare." *Id.*

<sup>44</sup> See *Marshall v. Barlow's, Inc.*, 436 U.S. 307, 314–15 (1978).

<sup>45</sup> *Id.* at 312.

<sup>46</sup> *Id.*

has generally imposed a number of requirements on searches and seizures. First, following the language of the Fourth Amendment,<sup>47</sup> the Court has recognized that the Fourth Amendment specifically prohibits only “unreasonable” searches and seizures.<sup>48</sup> Second, although the Fourth Amendment does not explicitly require a warrant as a prerequisite to a search, the Court has generally imposed a “warrant preference,” meaning that warrantless searches are presumptively unreasonable.<sup>49</sup> Finally, the Court has relatively strictly applied the Fourth Amendment requirements that warrants may not be issued absent a showing of probable cause and without specifying with particularity both the place to be searched and the things to be seized.<sup>50</sup>

In the administrative context, the Court applies these requirements quite differently. In *Camara*, the Court acted consistently with its overall jurisprudence in holding that the Fourth Amendment applies to administrative inspections, that such inspections require a warrant, and that administrative warrants must be based on probable cause.<sup>51</sup> However, the Court more loosely applied the concepts of “probable cause” and “particularity.” Outside of the administrative context, “probable cause” requires that the determination of probable cause be person or place specific.<sup>52</sup> For an arrest, the government must show reasonable cause to believe that a crime has been committed and that *the (particular) person to be arrested* committed it.<sup>53</sup> For a search, the government must show reasonable cause to believe that the fruits, instrumentalities, or evidence of crime exist, and can be found at *the (particular) place to be searched*.<sup>54</sup> In other words, as the Court stated in *Illinois v. Gates*,<sup>55</sup> the question is whether there is “a fair probability that contraband or evidence of a crime will be found in a particular place.”<sup>56</sup> Accordingly, the police do not have cause to search an individual simply because they can show that a high percentage of individuals in his (seedy) neighborhood sell or use drugs. Instead, they must show reasonable cause to believe that the particular person to be searched is in possession of drugs.

---

<sup>47</sup> U.S. CONST. amend. IV.

<sup>48</sup> *See, e.g., Camara v. Mun. Court*, 387 U.S. 523, 528–29 (1967).

<sup>49</sup> *Id.* The Court reasoned that “one governing principle, justified by history and by current experience, has consistently been followed: except in certain carefully defined classes of cases, a search of private property without proper consent is ‘unreasonable’ unless it has been authorized by a valid search warrant.” *Id.*; *see also Stoner v. California*, 376 U.S. 483 (1964); *United States v. Jeffers*, 342 U.S. 48 (1951); *McDonald v. United States*, 335 U.S. 451 (1948); *Agnello v. United States*, 269 U.S. 20 (1925).

<sup>50</sup> *See, e.g., Camara*, 387 U.S. at 528–29.

<sup>51</sup> *Id.* at 534–35.

<sup>52</sup> *Id.* at 534–35, 538.

<sup>53</sup> *See* RUSSELL L. WEAVER ET AL., PRINCIPLES OF CRIMINAL PROCEDURE 71 (4th ed. 2012) [hereinafter WEAVER ET AL. (4th ed.)].

<sup>54</sup> *Id.*

<sup>55</sup> 462 U.S. 213 (1983).

<sup>56</sup> *Id.* at 238; *see also Safford Unified Sch. Dist. No. 1 v. Redding*, 129 S. Ct. 2633, 2639 (2009).

In the administrative context, the Court does not require that the “probable cause” be particularized. In *Camara*,<sup>57</sup> a case in which an individual was fined for refusing to permit a warrantless administrative inspection of his residence for possible violations of a city housing code, the Court was confronted by a city ordinance which provided that

employees of the City departments or City agencies, so far as may be necessary for the performance of their duties, shall, upon presentation of proper credentials, have the right to enter, at reasonable times, any building, structure, or premises in the City to perform any duty imposed upon them by the Municipal Code.<sup>58</sup>

After holding that the Fourth Amendment requires a warrant and that the warrant must be based on probable cause, the Court then redefined the probable cause requirement so as not to require a “particularized” showing of probable cause in the administrative context.<sup>59</sup> For example, in enforcing a housing code, an agency need not show that a particular building is dilapidated and in need of inspection and possible repair.<sup>60</sup> Instead, the administrative agency can establish probable cause by showing that it has created reasonable legislative or administrative standards for inspections<sup>61</sup>—in other words, a reasonable plan for inspecting aging buildings. Such a plan may involve nothing more than the fact that it has created a reasonable inspection plan for the area or industry and that it is time to inspect the premises in question under that plan.<sup>62</sup> In order to inspect buildings in a dilapidated part of the city, a reasonable plan might include such standards as “the passage of time, the nature of the building (e.g., a multi-family apartment house), or the condition of the entire area, but [would] not necessarily depend upon specific knowledge of the condition of the particular dwelling.” Even though a particular building might have been completely updated, so that there is virtually no risk of dilapidation or deterioration, an administrative agency might still have “probable cause” to obtain a warrant to inspect it. In the Court’s view, this revised probable cause standard serves a valid purpose by guaranteeing “that a decision to search private property is justified by a reasonable governmental interest.”<sup>63</sup>

In altering the probable cause requirement, the Court emphasized several things. First, it balanced the need to search “against the invasion which the search entails.”<sup>64</sup> Second, the Court found that administrative inspections “have a long history of judicial

---

<sup>57</sup> 387 U.S. 523 (1967).

<sup>58</sup> *Id.* at 526.

<sup>59</sup> *Id.* at 538.

<sup>60</sup> *Id.* at 534.

<sup>61</sup> *Id.* at 538.

<sup>62</sup> *See* *Marshall v. Barlow’s, Inc.*, 436 U.S. 307, 323 (1978).

<sup>63</sup> *Camara*, 387 U.S. at 539.

<sup>64</sup> *Id.* at 537.



and public acceptance,”<sup>65</sup> and the Court doubted that “any other canvassing technique would achieve acceptable results.”<sup>66</sup> The Court noted that many conditions (i.e., faulty wiring) “are not observable from outside the building and indeed may not be apparent to the inexpert occupant himself.”<sup>67</sup> In addition, administrative inspections are not focused on the discovery of evidence, and “involve a relatively limited invasion of the urban citizen’s privacy.”<sup>68</sup>

The Court’s redefinition of probable cause in the administrative context might reasonably have been expected. In a number of prior cases, the Court had recognized the need for administrative inspections.<sup>69</sup> For example, in *Frank*, the Court stated that:

The growth of cities, the crowding of populations, the increased awareness of the responsibility of the state for the living conditions of its citizens, all have combined to create problems of the enforcement of minimum standards of far greater magnitude than the writers of these ancient inspection laws ever dreamed. Time and experience have forcefully taught that the power to inspect dwelling places, either as a matter of systematic area-by-area search or, as here, to treat a specific problem, is of indispensable importance to the maintenance of community health; a power that would be greatly hobbled by the blanket requirement of the safeguards necessary for a search of evidence of criminal acts. The need for preventive action is great, and city after city has seen this need and granted the power of inspection to its health officials; and these inspections are apparently welcomed by all but an insignificant few.<sup>70</sup>

Moreover, there is considerable pressure for administrative agencies to conduct “preventive” inspections.<sup>71</sup> Governmental officials could wait until individuals become sick or die before they inspect restaurants for clean and healthy conditions. Likewise, they could wait until an elevator crashes before conducting elevator safety inspections. However, for understandable reasons, governments prefer to do preventative inspections of restaurants and elevators in an effort to prevent sickness or injury.<sup>72</sup>

It is important not to read too much into the prevention justification. Outside of the administrative context, government may have a similarly compelling “need” to conduct

---

<sup>65</sup> *Id.*

<sup>66</sup> *Id.*

<sup>67</sup> *Id.*

<sup>68</sup> *Id.*

<sup>69</sup> *See, e.g., Frank v. Maryland*, 359 U.S. 360, 372 (1959).

<sup>70</sup> *Id.* at 371–72.

<sup>71</sup> *Id.* at 372.

<sup>72</sup> *See Camuglia v. City of Albuquerque*, 448 F.3d 1214, 1220 (10th Cir. 2006).

searches. As Justice Douglas recognized, dissenting in *Frank*, even though health inspections are important,

they are hardly more important than the search for narcotic peddlers, rapists, kidnapers, murderers, and other criminal elements. . . . Many today would think that the search for subversives was even more important than the search for unsanitary conditions. It would seem that the public interest in protecting privacy is equally as great in one case as in another. The fear that health inspections will suffer if constitutional safeguards are applied is strongly held by some.<sup>73</sup>

Nevertheless, *Camara*'s holding might have been better than the alternative. Because of the decision in *Frank*, there was a risk that the Court might simply have declared that the Fourth Amendment had no application to administrative inspections. In other words, rather than simply applying a lower standard of probable cause, the Court might have held that administrative inspections were not subject to the warrant requirement at all. As a result, administrative agencies could simply have chosen to inspect regulated entities at will and without a warrant. The requirement of a warrant, along with the redefined notions of probable cause and particularity, provided a substantial protection against administrative abuse. In theory, at least, that requirement prevents governmental officials from simply picking on their political enemies by subjecting them to frequent warrantless searches. In order to obtain a warrant, the agency must show that it has established a reasonable inspection plan, and that it is time to inspect this particular business under that plan.<sup>74</sup> Of course, the reality is that most administrative inspections are conducted without a warrant based on the consent of the person or business being searched.<sup>75</sup> Nevertheless, the warrant requirement, and the ability of a business to refuse consent, provides businesses with substantial protections if they choose to invoke that requirement.

#### *B. Exception for "Pervasively Regulated Businesses"*

A second area where the Court has chosen to single out administrative searches for special treatment involves the exception for so-called "pervasively regulated business[es]"<sup>76</sup> or "closely regulated industr[ies]" that have "long [been] subject to close supervision and inspection."<sup>77</sup> The Court has stated that these industries "have such a

---

<sup>73</sup> *Frank*, 359 U.S. at 382 (Douglas, J., dissenting).

<sup>74</sup> See *Camara v. Mun. Court*, 387 U.S. 523, 538 (1967).

<sup>75</sup> *Id.* at 539 ("[M]ost citizens allow inspections of their property without a warrant.").

<sup>76</sup> See *United States v. Biswell*, 406 U.S. 311, 316 (1972).

<sup>77</sup> See *Colonnade Catering Corp. v. United States*, 397 U.S. 72, 74, 77 (1970).

history of government oversight that [the owner can have] no reasonable expectation of privacy,”<sup>78</sup> and therefore the government can search them without a warrant.<sup>79</sup> As the Court has stated, “[W]hen an entrepreneur embarks upon such a business, he has voluntarily chosen to subject himself to a full arsenal of governmental regulation . . . of which any person who chooses to enter such a business must already be aware.”<sup>80</sup> Included are such enterprises as liquor sales and distribution,<sup>81</sup> firearms,<sup>82</sup> as well as underground and surface mines.<sup>83</sup> However, in *Marshall*, the Court refused to apply the exception to inspections conducted under the Occupational Safety and Health Act.<sup>84</sup>

Perhaps the outer limits of the “closely regulated” industry exception were established in *New York v. Burger*. That case involved a junkyard that dismantled cars and sold car parts.<sup>85</sup> Police officers from the New York City Police Department sought to inspect the junkyard pursuant to a New York law that authorized warrantless inspections of junkyards.<sup>86</sup> During the inspection of Burger’s business, the officers copied down the vehicle identification numbers on a number of vehicles that were subsequently determined to be stolen.<sup>87</sup> Based on this evidence, Burger was charged with possession of stolen property and operation of a junkyard in non-compliance with state law (requiring the maintenance of a “police book” etc.).<sup>88</sup> In upholding the search, the Court held that junkyards qualified as “closely regulated” businesses because, in addition to other requirements, junkyards were required to maintain a police book showing their acquisition and disposition of motor vehicles and vehicle parts, and they were required to make these records and inventory available for inspection by the police and other government agents.<sup>89</sup> The Court concluded that junkyards were “closely regulated” even though junkyards and vehicle dismantlers had not been in existence very long and therefore did not have a long history of regulation.<sup>90</sup> The Court viewed the industry as similar to secondhand shops and general junkyards which “long have been

---

<sup>78</sup> *Marshall v. Barlow’s, Inc.*, 436 U.S. 307, 313 (1978).

<sup>79</sup> *Id.*

<sup>80</sup> *Id.*

<sup>81</sup> *See Colonnade Catering Corp.*, 397 U.S. at 73–74.

<sup>82</sup> *See United States v. Biswell*, 406 U.S. 311, 311 (1978).

<sup>83</sup> *See Donovan v. Dewey*, 452 U.S. 594, 596 (1981).

<sup>84</sup> *Marshall*, 436 U.S. at 315 (“What is observable by the public is observable, without a warrant, by the Government inspector as well. The owner of a business has not, by the necessary utilization of employees in his operation, thrown open the areas where employees alone are permitted to the warrantless scrutiny of Government agents. That an employee is free to report, and the Government is free to use, any evidence of noncompliance with OSHA that the employee observes furnishes no justification for federal agents to enter a place of business from which the public is restricted and to conduct their own warrantless search.” (footnotes omitted)).

<sup>85</sup> 482 U.S. 691 (1987).

<sup>86</sup> *Id.* at 693.

<sup>87</sup> *Id.* at 695.

<sup>88</sup> *Id.* at 704.

<sup>89</sup> *Id.* at 703–04.

<sup>90</sup> *Id.* at 705–07.

subject to regulation.”<sup>91</sup> As a result, the Court found that junkyard owners engaged in dismantling have a reduced expectation of privacy.<sup>92</sup>

After concluding that dismantling was a closely regulated business, the Court examined the New York statute to determine whether it met the three criteria for warrantless inspections of closely regulated businesses.<sup>93</sup> The Court found a “substantial interest in regulating the vehicle-dismantling and automobile-junkyard industry because motor vehicle theft has increased in the State and because the problem of theft is associated with this industry.”<sup>94</sup> The State could reasonably find that “regulation of the vehicle-dismantling industry reasonably serves the State’s substantial interest in eradicating automobile theft.”<sup>95</sup> It reasoned that “stolen cars and parts often pass quickly through an automobile junkyard, [and] ‘frequent’ and ‘unannounced’ inspections are necessary in order to detect them.”<sup>96</sup> In addition, the statute provided a “constitutionally adequate substitute for a warrant.”<sup>97</sup> The statute “inform[ed] the operator of a vehicle dismantling business that inspections [would] be made on a regular basis” and provided details regarding the scope of the inspections.<sup>98</sup> Finally, the Court held that the “time, place, and scope”<sup>99</sup> of the inspection was limited “to plac[ing] appropriate restraints upon the discretion of the inspecting officers.”<sup>100</sup> Inspections were limited to regular business hours, and the scope of the search was narrowly defined: The inspectors could examine the records, as well as “any vehicles or parts of vehicles which are subject to the record keeping requirements of this section and which are on the premises.”<sup>101</sup>

The *Burger* decision was extraordinary because the search did not involve a typical administrative inspection by a traditional administrative agency, but instead involved police searches for evidence of criminal activity. Nevertheless, the Court upheld the searches as administrative inspections: “[A] State can address a major social problem *both* by way of an administrative scheme *and* through penal sanctions.”<sup>102</sup> “So long as a regulatory scheme is properly administrative, it is not rendered illegal by the fact that the inspecting officer has the power to arrest individuals for violations other than those created by the scheme itself.”<sup>103</sup>

Justice Brennan, dissenting, questioned whether vehicle dismantlers really qualify as closely regulated businesses.<sup>104</sup> He noted that the regulations governing their

---

<sup>91</sup> *Id.* at 706.

<sup>92</sup> *Id.* at 707.

<sup>93</sup> *Id.* at 708–12.

<sup>94</sup> *Id.* at 708.

<sup>95</sup> *Id.* at 709.

<sup>96</sup> *Id.* at 710.

<sup>97</sup> *Id.* at 711 (quoting *Donovan v. Dewey*, 452 U.S. 594, 603 (1981)).

<sup>98</sup> *Id.* (citing *Donovan*, 452 U.S. at 605).

<sup>99</sup> *Id.* (quoting *United States v. Biswell*, 406 U.S. 311, 315 (1972)).

<sup>100</sup> *Id.* (citing *Donovan*, 452 U.S. at 605).

<sup>101</sup> *Id.* at 711–12.

<sup>102</sup> *Id.* at 712.

<sup>103</sup> *Id.* at 717.

<sup>104</sup> *Id.* at 718 (Brennan, J., dissenting).

existence were not extensive: “Few substantive qualifications are required of an aspiring vehicle dismantler; no regulation governs the condition of the premises, the method of operation, the hours of operation, the equipment utilized, etc. This scheme stands in marked contrast to, *e. g.*, [sic] the mine safety regulations relevant in *Donovan v. Dewey*.”<sup>105</sup> In addition, he questioned whether there was any assurance that inspections would be conducted on a regular basis, or at all.<sup>106</sup> In other words, the statute provided no “constitutionally adequate substitute for a warrant.”<sup>107</sup> Finally, he noted that the law authorized searches intended solely to uncover evidence of criminal acts: “[T]he State has used an administrative scheme as a pretext to search without probable cause for evidence of criminal violations.”<sup>108</sup>

### *C. Emergency Exception*

The Court has also recognized that there are a number of situations in the administrative context when warrantless inspections are constitutionally permissible. For example, a warrant is not required in “emergency situations” involving the seizure of unwholesome food, smallpox vaccinations, health quarantines, or the summary destruction of tubercular cattle.<sup>109</sup>

## II. THE ADMINISTRATIVE EXCEPTION AND PERSONAL PRIVACY: WARNING SIGNALS FROM THE BORDER EXCEPTION DEBATES

It is tempting to view the Court’s Fourth Amendment jurisprudence as *sui generis* as it has been applied in the administrative context. In other words, or so the argument goes, the administrative exception applies in limited contexts that often (although not exclusively) affect only businesses.<sup>110</sup> The difficulty is that, in a modern society, involving technological advancement and innovation, the dividing line between administrative searches and “other” searches is not clear or well-defined. In one area of the law—border searches—the administrative exception has the potential to dramatically limit individual privacy.

---

<sup>105</sup> *Id.* at 721.

<sup>106</sup> *Id.* at 722.

<sup>107</sup> *Id.* (quoting *Donovan v. Dewey*, 452 U.S. 594, 603 (1981)).

<sup>108</sup> *Id.* at 725.

<sup>109</sup> See *Camara v. Mun. Court*, 387 U.S. 523, 539 (1967). The Court recognized the importance of “prompt [administrative] inspections, even without a warrant, . . . in emergency situations.” *Id.* (citing *N. Am. Cold Storage Co. v. City of Chicago*, 211 U.S. 306 (1908) (seizure of unwholesome food); *Compagnie Francaise de Navigation a Vapeur v. La. State Bd. of Health*, 186 U.S. 380 (1902) (health quarantine); *Kroplin v. Truax*, 165 N.E. 498 (Ohio 1929) (summary destruction of tubercular cattle)).

<sup>110</sup> See, *e.g.*, David A. Christensen, *Warrantless Administrative Searches Under Environmental Laws: The Limits to EPA Inspectors’ Statutory Invitation*, 26 ENVTL. L. 1019, 1033 (1996) (arguing that the Supreme Court’s decisions regarding administrative searches of commercial property reveal that warrantless inspection “is reasonable only under statutes that target specific industries”).

The exception for border searches illustrates the potential privacy implications of the administrative exception. The U.S. Supreme Court has held that the government's power is at its zenith at the border and that the government retains broad powers to search those who seek to enter or transport goods into the country.<sup>111</sup> As the Court stated in *United States v. Flores-Montano*, "searches made at the border, pursuant to the longstanding right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border."<sup>112</sup>

Undoubtedly, the government has substantial justifications for stopping individuals at the border, as well as for making inquiries and conducting searches. Government has the right to ensure that those seeking to enter the United States are actually authorized to do so and therefore to demand that those seeking entry prove their right to do so.<sup>113</sup> In addition, the United States has always retained the right to ensure that contraband and potentially dangerous items do not enter the United States.<sup>114</sup> As a result, the United States has reserved to itself the power to inspect bags and other items brought into the United States.<sup>115</sup>

Because of this attitude, the Court has regarded border searches as "routine"<sup>116</sup> and has generally allowed customs officials to exercise broad powers.<sup>117</sup> For example, customs officials may search individuals and their luggage at the border whether or not they have particularized cause to suspect wrongdoing.<sup>118</sup> As the Court recognized in *United States v. Thirty-Seven Photographs*<sup>119</sup>:

---

<sup>111</sup> See *United States v. Flores-Montano*, 541 U.S. 149, 152–53 (2004).

<sup>112</sup> *Id.* (quoting *United States v. Ramsey*, 431 U.S. 606, 616 (1977) (internal quotation marks omitted)).

<sup>113</sup> See *Ramsey*, 431 U.S. at 618 ("Travelers 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, 154 (1925))); *Almeida-Sanchez v. United States*, 413 U.S. 266, 272 (1973) (noting that it is "without doubt" that the power to exclude aliens "can be effectuated by routine inspections and searches of individuals or conveyances seeking to cross our borders").

<sup>114</sup> See *Ramsey*, 431 U.S. at 618–19.

<sup>115</sup> *Id.*

<sup>116</sup> *Id.* at 619.

<sup>117</sup> See *United States v. Montoya de Hernandez*, 473 U.S. 531, 538 (1985) ("Routine searches of the persons and effects of entrants are not subject to any requirement of reasonable suspicion, probable cause, or warrant . . ."); *United States v. 12 200-Ft. Reels of Super 8mm. Film*, 413 U.S. 123, 125 (1973) ("Import restrictions and searches of persons or packages at the national borders rest on different considerations and different rules of constitutional law from domestic regulations. The Constitution gives Congress broad, comprehensive powers '[t]o regulate Commerce with foreign Nations.' Art. I, § 8, cl. 3. Historically such broad powers have been necessary to prevent smuggling and to prevent prohibited articles from entry.").

<sup>118</sup> See *Montoya de Hernandez*, 473 U.S. at 538; *Almeida-Sanchez*, 413 U.S. at 272–73.

<sup>119</sup> 402 U.S. 363 (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. Customs officers characteristically inspect luggage and their power to do so is not questioned in this case; it is an old practice and is intimately associated with excluding illegal articles from the country.<sup>120</sup>

The Court has suggested that it might impose more rigorous requirements on searches that are deemed to be “unreasonable” because of the “particularly offensive manner” in which they are conducted.<sup>121</sup> Included within these latter searches are strip, body-cavity, or involuntary X-ray searches.<sup>122</sup>

The difficulty is that, as the nature of the “items” crossing international borders has changed as technology has changed, the Court's jurisprudence has not.<sup>123</sup> Instead of carrying ordinary goods across U.S. borders, individuals now carry many different types of electronic devices with them. In addition to iPhones and cellphones, it is not uncommon for international travelers to go through customs carrying digital cameras, laptop and notebook computers, Kindles (and other book readers), and iPads.<sup>124</sup> Many of these items contain not only large amounts of personal information but also highly confidential information.<sup>125</sup> Moreover, since many electronic devices are connected to servers or to cloud storage systems, it is possible to access an extraordinary quantity of information through these devices.<sup>126</sup>

---

<sup>120</sup> *Id.* at 376.

Border searches, then, from before the adoption of the Fourth Amendment, have been considered to be “reasonable” by the single fact that the person or item in question had entered into our country from outside. There has never been any additional requirement that the reasonableness of a border search depended on the existence of probable cause. This longstanding recognition that searches at our borders without probable cause and without a warrant are nonetheless “reasonable” has a history as old as the Fourth Amendment itself. We reaffirm it now.

*Ramsey*, 431 U.S. at 619 (footnote omitted).

<sup>121</sup> *See Ramsey*, 431 U.S. at 618 n.13.

<sup>122</sup> *See Montoya de Hernandez*, 473 U.S. at 541 n.4; *see also* *United States v. Sandler*, 644 F.2d 1163, 1169 (5th Cir. 1981) (holding that the permissibility of a warrantless pat-down and search of outer clothing should not be necessarily extended to more intrusive searches).

<sup>123</sup> *See, e.g., United States v. Cotterman*, 709 F.3d 952, 956–57 (9th Cir. 2013), *petition for cert. filed* Aug. 5, 2013 (acknowledging that it was prescient to incorporate “papers” within the Fourth Amendment's purview, but that people crossing American borders today, as “denizens of a digital world,” carry many electronic devices).

<sup>124</sup> *Id.* at 956.

<sup>125</sup> *Id.*

<sup>126</sup> *Id.* at 965.

Does the federal government have an absolute right to search these electronic devices simply because they are being carried into the United States? One can argue that the “writings” contained on electronic devices are no different from written manuscripts that might have entered the country in eighteenth or nineteenth centuries, and that might have been subject to search at that time. On the other hand, one can also argue that electronic devices are distinct in important respects. For one thing, electronic devices can store far more information. If the government has the “right” to search all electronic devices, then legitimate questions might be raised regarding the scope of that right. Are customs officials only allowed to do a cursory inspection? Alternatively, can they seize electronic devices and send them off to forensics labs for detailed analysis of their content? Can they copy electronic files from a laptop and review them at their leisure?

In the physical search cases, the Court has held that customs officials have broad authority to conduct extensive border searches.<sup>127</sup> For example, in *Flores-Montano*, when customs officials believed that Flores-Montano was carrying contraband in the gas tank of his automobile, the Court held that those officials could remove and disassemble the gas tank.<sup>128</sup> The Court flatly stated that an individual’s expectation of privacy is lower at the border because the Court has “long recognized that automobiles seeking entry into this country may be searched.”<sup>129</sup> The Court viewed the search of a gas tank as no more intrusive than the search of an automobile’s passenger compartment and concluded “that the disassembly and reassembly of [the] gas tank [did not involve] a significant deprivation” of property even though the vehicle could have been damaged.<sup>130</sup> The Court believed that any damage that the search caused could have been “justified by the Government’s paramount interest in protecting the border.”<sup>131</sup> The Court left open the possibility that some searches of property could be “so destructive as to require a different result.”<sup>132</sup>

#### *A. Border Searches for Information Making Accompanied Crossings of the U.S. Border*

Might similar principles justify inspection and examination of the information contained on electronic devices? In *United States v. Adams*,<sup>133</sup> a lower court held that the border search doctrine gives the government the power to search through private files and documents.<sup>134</sup> In that case, governmental officials confiscated and searched Adams’ address book, which they found on a small private plane that flew into the United States.<sup>135</sup> The search revealed the name of a co-conspirator in the drug-smuggling

<sup>127</sup> See *supra* notes 113–20 and accompanying text.

<sup>128</sup> 541 U.S. 149, 150–51, 155 (2004).

<sup>129</sup> *Id.* at 154.

<sup>130</sup> *Id.* at 154–55.

<sup>131</sup> *Id.* at 155.

<sup>132</sup> *Id.* at 155–56.

<sup>133</sup> 1 F.3d 1566 (11th Cir. 1993).

<sup>134</sup> *Id.* at 1574, 1577.

<sup>135</sup> *Id.* at 1577.



operation.<sup>136</sup> The Court held that a warrantless search of an airplane that had entered the United States was a valid border search and that government had broad authority to search the plane.<sup>137</sup>

The U.S. government's view is that there should be no significant distinction, in terms of the analytical approach, between looking at an address book and searching through a traveler's computer files.<sup>138</sup> In its assessment, the Department of Homeland Security (DHS) flatly states that:

The advent of compact, large capacity, and inexpensive electronic devices, such as laptop computers, thumb drives, compact disks (CD), digital versatile disks (DVD), cell phones, subscriber identity module (SIM) cards, digital cameras, and other devices capable of storing electronic information (hereinafter "electronic devices") has enabled the transportation of large volumes of information, some of which is highly personal in nature. When these devices are carried by a traveler crossing the U.S. border, these and all other belongings are subject to search by the U.S. Department of Homeland Security (DHS) to ensure the enforcement at the border of immigration, customs, and other federal laws.<sup>139</sup>

Even though the DHS recognizes that searches of electronic devices raise significant privacy concerns,<sup>140</sup> the DHS believes that such searches are justified by

---

<sup>136</sup> *Id.*

<sup>137</sup> It is clear that the search was a valid border search, one for which a warrant was not required. "The fact that one is in the process of crossing an international boundary provides sufficient reason in itself to permit a search for aliens or contraband, without the presence of any other circumstance that would normally have to attend the requirements of the Fourth Amendment." *United States v. Moreno*, 778 F.2d 719, 721 (11th Cir. 1985) (quoting *United States v. McDaniel*, 463 F.2d 129, 132 (5th Cir. 1972)). "Such a search is reasonable for Fourth Amendment purposes simply because a border has been crossed. The mere fact that in this case the search did not technically occur at the border is irrelevant; the point where [the defendant] ultimately landed his aircraft is construed as the functional equivalent of the border."

*Id.*; see *United States v. Hewitt*, 724 F.2d 117, 119 (11th Cir. 1984); see also *United States v. Ramsey*, 431 U.S. 606, 616 (1977).

<sup>138</sup> See, e.g., HOMELAND SECURITY ASSESSMENT, *supra* note 29, at 2.

<sup>139</sup> *Id.*

<sup>140</sup> There are two basic privacy concerns at the heart of DHS searching electronic devices at the border. The first is the propriety of the border search, as in whether the search is lawful under U.S. law. The legal foundation for border searches of any object at the border, regardless of its type, capacity, or format, is well-established and is discussed in detail below.

the fact that illegal information can be carried across the nation's borders on electronic devices.<sup>141</sup>

How much power does the DHS possess regarding these computer devices? The Department takes the position that it has broad authority to search and inspect them. For one thing, even when the DHS inspects an electronic device, it is not always required to inform the traveler of this fact.<sup>142</sup> In addition, the DHS takes the position that it has the authority to detain an electronic device for further inspection, or to copy the information contained on that device for later review and inspection.<sup>143</sup> Ordinarily, this

---

The second and more central privacy concern is the sheer volume and range of types of information available on electronic devices as opposed to a more traditional briefcase or backpack. In the past, someone might bring a briefcase or similar accessory across the border that contains pictures of their friends or family, work materials, personal notes or journals, or any other type of personal information. Because of the availability of electronic information storage and the capacity for comfortable portability, the amount of personal and business information that can be hand-carried by a single individual has increased exponentially. Where someone may not feel that the inspection of a briefcase would raise significant privacy concerns because the volume of information to be searched is not great, that same person may feel that a search of their laptop increases the possibility of privacy risks due to the vast amount of information potentially available on electronic devices.

*Id.* (footnote omitted).

<sup>141</sup> At the same time that individuals seek to lawfully transport electronic information with no link to criminal activity across the border, criminals attempt to bring merchandise contrary to law into the United States using the same technology. The use of electronic devices capable of storing information relating to criminal activities has been established as the latest method for smuggling these materials. As the world of information technology evolves, the techniques used by CBP and ICE and other law enforcement agencies must also evolve to identify, investigate, and prosecute individuals using new technologies in the perpetration of crimes. Failure to do so would create a dangerous loophole for criminals seeking to import or export merchandise contrary to law.

*Id.* at 2–3.

<sup>142</sup> *Id.* at 4 (“In many instances, CBP and ICE conduct border searches of electronic devices with the knowledge of the traveler. However, in some situations it is not practicable for law enforcement reasons to inform the traveler that his electronic device has been searched.”).

<sup>143</sup> A detention occurs when CBP or ICE determines that the devices need to be kept for further examination to determine if there is probable cause to seize as evidence of a crime and/or for forfeiture. This is a temporary detention of the device during an ongoing border search. Many factors may result in a detention, for example, time constraints due to connecting flights, the large volume of information to be examined, the need to use off-site tools and expertise during the search (e.g., an ICE forensic lab), or the need for translation or other specialized services to understand the information on the device. In a detention, CBP or ICE will keep either the original device (e.g., the laptop) or an exact duplicate copy of the

detention should not exceed five days, but the DHS reserves the right to share contents stored on the device with other administrative agencies, and to retain electronic devices for up to thirty days.<sup>144</sup> Detentions beyond thirty days “must be approved by an ICE supervisor, approved again every 15 days thereafter, and documented in the appropriate ICE record systems.”<sup>145</sup> Instead of detaining a device, the DHS can elect to copy the electronic contents for later review.<sup>146</sup> In some instances, the DHS has the power to destroy electronic information.<sup>147</sup> In the final analysis, such searches, detentions, and copying are relatively routine:

As federal criminal investigators, ICE Special Agents are empowered to make investigative decisions based on the particular facts and circumstances of each case. The decision to detain or seize electronic devices or detain, seize, or copy information therefrom is a typical decision a Special Agent makes as part of his or her basic law enforcement duties.<sup>148</sup>

Thus far, there is some disagreement between the cases, but some decisions suggest that the DHS has broad authority to inspect electronic devices. In *United States v.*

---

information stored on the device, so as to allow the traveler to proceed with the original device. Once the border search has concluded, the device will be returned to the traveler unless there is probable cause to seize the device. Any copies of the information in the possession of CBP or ICE will be destroyed unless retention of the information is necessary for law enforcement purposes and appropriate within CBP or ICE Privacy Act systems of records.

*Id.* at 5.

<sup>144</sup> *Id.* at 7 (“In most cases, when CBP or ICE keeps the device and the traveler leaves the port without it, the electronic device is considered ‘detained.’ For CBP, the detention of devices ordinarily should not exceed five (5) days, unless extenuating circumstances exist.” (footnote omitted)).

<sup>145</sup> *Id.* at 9 (footnote omitted).

<sup>146</sup> Instead of detaining the electronic device, CBP or ICE may instead copy the contents of the electronic device for a more in-depth border search at a later time. For CBP, the decision to copy data contained on an electronic device requires supervisory approval. Copying may take place where CBP or ICE does not want to alert the traveler that he is under investigation; where facilities, lack of training, or other circumstances prevent CBP or ICE from performing the search at secondary inspection; or where the traveler is unwilling or is unable to assist, or it is not prudent to allow the traveler to assist in the search (such as providing a password to log on to a laptop).

*Id.* at 8 (footnote omitted).

<sup>147</sup> *Id.* at 10 (“Detained electronic information that is destroyed is not merely deleted, but forensically wiped, which entails writing over the information multiple times to ensure it cannot be accessed again. Once the electronic copy is forensically wiped, a record of the destruction is documented in the TECS Report of Investigation (ROI), as appropriate.” (footnote omitted)).

<sup>148</sup> *Id.* at 8.

*Cotterman*, a husband and wife, who were traveling under U.S. passports, tried to cross from Mexico into the United States.<sup>149</sup> Customs officials decided to seize their laptops and digital cameras and send those devices to a forensics lab in another city for forensic examination.<sup>150</sup> Although the husband offered to help customs officials access the laptops by providing passwords, the officials declined for fear that defendant would tamper with or delete content, and also because they feared that “the laptops might be ‘booby trapped’” or that “there might be files [they] would be unable to see even with full access to the laptops.”<sup>151</sup> Although defendants were allowed entry into the United States, their electronics equipment was shipped to Tuscon (170 miles away), a place where defendants happened to be going, and two of the laptops were held for four days.<sup>152</sup>

It is one thing if courts strictly circumscribe searches of computers and other digital equipment based on a warrant and probable cause. However, in *Cotterman*, customs officials did not obtain a warrant.<sup>153</sup> Moreover, although the government had a basis for believing that the husband might be carrying child pornography on his electronic devices, the government freely admitted that it did not have a “particularized suspicion” of criminal activity.<sup>154</sup> Indeed, the government argued that it was not required to show cause because the border-search doctrine gave it the power to seize the computer, carry it to a distant location for analysis, and complete the search.<sup>155</sup> As a result, the government argued that its actions should be regarded as “reasonable” under the Fourth Amendment.<sup>156</sup>

The opinions in the *Cotterman* case—the trial court opinion and the appellate opinion—offer much insight into the conflicting ways that courts evaluate this type of case. In sustaining the seizure, the trial court gave short shrift to Cotterman’s objections.<sup>157</sup> The court began by reaffirming the breadth of governmental power under the border-search doctrine:

We need not dwell long on the general scope of the Government’s border search power. It is well-established that the sovereign need not make any special showing to justify its search of persons and property at the international border. Rather, it is the traveler who

---

<sup>149</sup> 637 F.3d 1068 (9th Cir. 2011), *rev’d* 709 F.3d 952 (9th Cir. 2013).

<sup>150</sup> *Id.* at 1071–72. The seizure was based on information found in a government database, indicating that Cotterman had been convicted of two counts of lewd and lascivious conduct upon a child, and three counts of child molestation, and suggesting that customs officials be on the “lookout” for child pornography. *Id.*

<sup>151</sup> *Id.*

<sup>152</sup> *Id.* at 1070, 1072.

<sup>153</sup> *Id.* at 1071–72.

<sup>154</sup> *Id.* at 1071, 1074.

<sup>155</sup> *Id.* at 1074.

<sup>156</sup> *Id.* at 1081.

<sup>157</sup> *Id.* at 1076.

must demonstrate he is entitled to cross our borders and to bring with him whatever he may wish to carry.<sup>158</sup>

Indeed, the court made it clear that it would have routinely upheld the inspection of Cotterman's computer had the inspection been done at the international border.<sup>159</sup> In other words, customs officials could have searched Cotterman's electronic information on his laptops and cameras.

The court then examined whether customs officials could seize Cotterman's electronic equipment at the border, transport it to another city for forensics analysis, and ultimately hold on to it for several days.<sup>160</sup> Cotterman claimed that the actions of customs officials were unreasonable and therefore a violation of the Fourth Amendment.<sup>161</sup> The court disagreed, noting that the government has broad authority to seize property at the nation's borders.<sup>162</sup> The court also held that a traveler does not have a reasonable expectation of privacy in his luggage when he crosses the nation's borders.<sup>163</sup> Since Cotterman was never allowed to enter the country with his electronic equipment, he never regained his expectation of privacy with regard to that equipment.<sup>164</sup> "Quite to the contrary, the Court has indicated that travelers should expect intrusions and delay

---

<sup>158</sup> *Id.* at 1074–75 (citations omitted).

<sup>159</sup> *Id.* at 1075–76.

<sup>160</sup> *Id.* at 1076–79.

<sup>161</sup> *Id.* at 1076.

<sup>162</sup> As a preliminary matter, we readily dispense with Cotterman's claim—and the first of three principal arguments relied upon by the dissent—that the Government may search property at the border, but is powerless to seize property to adequately conduct its search absent some particularized suspicion. Quite to the contrary, we note that the Supreme Court has explicitly recognized that the Government possesses inherent authority to seize property at the international border without suspicion: "Since the founding of our Republic, Congress has granted the Executive plenary authority to conduct routine searches *and seizures* at the border, *without probable cause or a warrant*, in order to regulate the collection of duties and to prevent the introduction of contraband into this country."

*Id.* at 1075 n.9 (citations omitted) (quoting *United States v. Montoya de Hernandez*, 473 U.S. 531, 537 (1985)).

<sup>163</sup> *Id.* at 1077; *see also* *United States v. Flores-Montano*, 541 U.S. 149, 155 n.3 (2004) (rejecting the contention that there is a "Fourth Amendment right not to be subject to delay at the international border"); *United States v. Montoya de Hernandez*, 473 U.S. 531, 537 (1985) ("[T]he Executive [has] plenary authority to conduct routine searches and seizures at the border . . ."); *United States v. Ross*, 456 U.S. 798, 823 (1982) ("The luggage carried by a traveler entering the country may be searched at random by a customs officer . . . no matter how great the traveler's desire to conceal the contents may be."); *United States v. Thirty-Seven Photographs*, 402 U.S. 363, 376 (1971) ("But 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.").

<sup>164</sup> *Cotterman*, 637 F.3d at 1077.

in order to satisfy the Government's sovereign interest in protecting our borders from those who would wish to do us harm."<sup>165</sup> The court refused to impose any additional requirements as a precondition to a decision to remove property away from the border for further inspection.<sup>166</sup>

The trial court decision in *Cotterman* was subsequently overturned by the Ninth Circuit in a decision that recognized the privacy implications raised by the situation.<sup>167</sup> The court of appeals sought to balance the government interest in protecting the borders against the individual interest in privacy, and to determine whether the actions of customs officials should be regarded as "reasonable," as required by the Fourth Amendment.<sup>168</sup> In light of this balancing, the court held that border agents are free to do a quick scan of electronic devices, including looking at the contents.<sup>169</sup> However, the court suggested that the forensic examination of the computer at a remote site could not be regarded as an "extended border search"<sup>170</sup> and therefore required greater cause.<sup>171</sup>

---

<sup>165</sup> *Id.* at 1078.

<sup>166</sup> *Id.*

<sup>167</sup> *United States v. Cotterman*, 709 F.3d 952 (9th Cir. 2013).

<sup>168</sup> *Id.* at 960–61.

<sup>169</sup> [T]he legitimacy of the initial search of Cotterman's electronic devices at the border is not in doubt. Officer Alvarado turned on the devices and opened and viewed image files while the Cottermans waited to enter the country. It was, in principle, akin to the search in *Seljan*, where we concluded that a suspicionless cursory scan of a package in international transit was not unreasonable. 547 F.3d at 1004. Similarly, we have approved a quick look and unintrusive search of laptops. *United States v. Arnold*, 533 F.3d 1003, 1009 (9th Cir. 2008) (holding border search reasonable where "CBP officers simply 'had [traveler] boot [the laptop] up, and looked at what [he] had inside.'" (second alteration in original)). Had the search of Cotterman's laptop ended with Officer Alvarado, we would be inclined to conclude it was reasonable even without particularized suspicion.

*Id.*

<sup>170</sup> Although the semantic moniker "extended border search" may at first blush seem applicable here, our jurisprudence does not support such a claim. We have "define[d] an extended border search as any search away from the border where entry is not apparent, but where the dual requirements of reasonable certainty of a recent border crossing and reasonable suspicion of criminal activity are satisfied." *United States v. Guzman-Padilla*, 573 F.3d 865, 878–79 (9th Cir. 2009). . . . Cotterman's case is different. Cotterman was stopped and searched at the border. Although he was allowed to depart the border inspection station after the initial search, some of his belongings, including his laptop, were not. The follow-on forensic examination was not an "extended border search." A border search of a computer is not transformed into an extended border search simply because the device is transported and examined beyond the border.

*Id.* at 961.

<sup>171</sup> *Id.* at 961–62.

In imposing higher requirements, the court emphasized the amount of personal information carried by international travelers on computers,<sup>172</sup> and the potentially confidential and sensitive nature of that information.<sup>173</sup> As a result, the court concluded that a finding of “reasonable suspicion” of criminal activity is a prerequisite to a forensic examination of a computer.<sup>174</sup> However, the court also concluded that customs officials did, in fact, have a reasonable suspicion that Cotterman was involved in criminal activity.<sup>175</sup>

*United States v. McAuley*<sup>176</sup> is another trial court decision that broadly applies the border-search exception to electronics equipment. In that case, the defendant, who was suspected of being involved in child pornography, arrived at the U.S. border carrying a zip drive, two external hard drives, and a laptop.<sup>177</sup> There was some dispute regarding whether the defendant consented to the search of his computer; the defendant claimed that he did not.<sup>178</sup> Nevertheless, the subsequent search revealed the existence of child pornography on an external hard drive.<sup>179</sup> The defendant claimed that a computer search is “non-routine” and that probable cause or reasonable suspicion should be required as a prerequisite to a search of a computer’s contents.<sup>180</sup> The court reaffirmed the idea that “routine” border searches lie squarely within the scope of governmental authority.<sup>181</sup>

---

<sup>172</sup> Electronic devices are capable of storing warehouses full of information. The average 400—gigabyte laptop hard drive can store over 200 million pages—the equivalent of five floors of a typical academic library. Even a car full of packed suitcases with sensitive documents cannot hold a candle to the sheer, and ever-increasing, capacity of digital storage.

*Id.* at 964 (citations omitted).

<sup>173</sup> The nature of the contents of electronic devices differs from that of luggage as well. Laptop computers, iPads and the like are simultaneously offices and personal diaries. They contain the most intimate details of our lives: financial records, confidential business documents, medical records and private emails. This type of material implicates the Fourth Amendment’s specific guarantee of the people’s right to be secure in their “papers.” U.S. Const. amend. IV. The express listing of papers “reflects the Founders’ deep concern with safeguarding the privacy of thoughts and ideas—what we might call freedom of conscience—from invasion by the government.” *Seljan*, 547 F.3d at 1014 (Kozinski, C.J., dissenting).

*Id.*

<sup>174</sup> *Id.* at 968.

<sup>175</sup> *Id.* at 970.

<sup>176</sup> 563 F. Supp. 2d 672 (W.D. Tex. 2008), *aff’d*, 420 F. App’x 400 (5th Cir. 2011) (affirming on the theory that McAuley consented to the search).

<sup>177</sup> *Id.* at 674.

<sup>178</sup> *Id.* at 674–75.

<sup>179</sup> *Id.*

<sup>180</sup> *Id.* at 676.

<sup>181</sup> The border search doctrine is one of the few exceptions that allow a warrantless search at a port of entry. “Agents may conduct a ‘routine’ search—one that does not seriously invade a traveler’s privacy at the

Moreover, the court defined the following activities as falling squarely within the scope of that “routine” authority, which “require no justification other than the person’s decision to cross our national boundary”: “ordinary pat-downs and frisks, removal of outer garments and shoes, and the emptying of pockets, wallets, and purses.”<sup>182</sup> However, a “non-routine” search (such as a body-cavity search or a strip search) requires “reasonable suspicion” that the individual is involved in criminal activity.<sup>183</sup> Defendant argued that a computer search is like a strip search (or other non-routine searches) because computers contain private information.<sup>184</sup> However, the court viewed a computer search as more analogous to a search of an automobile or its contents.<sup>185</sup> The court justified its decision as follows:

Incredible amounts of personal and sensitive information are already subject to scrutiny at ports of entry in peoples’ wallets, purses, locked glove boxes, and locked containers or luggage. People carry personal items such as Social Security cards; state and federal identification cards; medicines and medical records; names and addresses of family and associates; day planners with itineraries and travel documents; credit cards; check books and registries; business cards; photographs; and membership cards. All of these items are already subject to routine border searches. A computer is simply an inanimate object made up of microprocessors and wires which happens to efficiently condense and digitize the information reflected by the items listed above. The fact that a computer may take such personal information and digitize it does not alter the Court’s analysis.<sup>186</sup>

Moreover, to the court, it made no difference that the computer was password protected.<sup>187</sup>

---

international border or its functional equivalent without probable cause, a warrant, or any suspicion to justify the search.” *Roberts*, 274 F.3d at 1011. The key variable used to determine whether a search is “routine” is “the invasion of the privacy and dignity of the individual.”

*Id.*

<sup>182</sup> *Id.* (quoting *United States v. Sandler*, 644 F.2d 1163, 1169 (5th Cir. 1981)).

<sup>183</sup> *See Sandler*, 644 F.2d at 1169 n.6.

<sup>184</sup> *McAuley*, 563 F. Supp. 2d at 677.

<sup>185</sup> *Id.*

<sup>186</sup> *Id.* at 678 (citation omitted); *see also* *United States v. Cardenas*, 9 F.3d 1139, 1148 n.3 (5th Cir. 1993).

<sup>187</sup> While the Defendant’s computer was password protected, it too does not effect this Court’s analysis. A password on a computer does not automatically convert a routine search into a non-routine search. A password is simply a digital lock. Locks are usually present on luggage and briefcases,



So, while the court of appeals' decision in *Cotterman* suggested that border searches should be limited in scope, absent proof of cause for a more extended search, two trial court decisions go the other way. Moreover, the DHS takes the position that it has broad authority under the border search exception.<sup>188</sup>

*B. Border Searches for Information Making Unaccompanied Crossings of the U.S. Border*

The border-search doctrine becomes even more problematic if it is applied to any physical object or communication that crosses the United States' international borders, and today many electronic communications cross those borders every day. Some of that information moves entirely electronically. The most obvious sources of such movement are e-mails or Skype communications sent across the border. Do governmental officials have the right to "inspect" and review all e-mails or other communications that cross the U.S. border?

In theory, it is arguable whether the Fourth Amendment applies to international Internet communications at all. In *Cotterman*, the trial court held that there is no reasonable expectation of privacy in items crossing the international borders.<sup>189</sup> Before the Fourth Amendment applies at all, there must be a "search" or a "seizure" within the meaning of the Fourth Amendment.<sup>190</sup> The U.S. Supreme Court has struggled to define the term "search" in an electronic era.<sup>191</sup> "[W]hen the Fourth Amendment was drafted and ratified, the state of surveillance technology was relatively crude and simplistic, and the ability of the government to pry into the lives of private citizens was much more circumscribed."<sup>192</sup> In drafting the Fourth Amendment, the new Americans were focused on abuses committed by the British during the colonial period, in particular their use of writs of assistance and general warrants to make actual physical searches of houses, persons, papers, and effects.<sup>193</sup> Moreover, the Framers of the Fourth Amendment could hardly have envisioned the surveillance technologies that would later be developed or

---

yet those items are subject to "routine" searches at ports of entry all the time.

*McAuley*, 563 F. Supp. 2d at 679.

<sup>188</sup> See HOMELAND SECURITY ASSESSMENT, *supra* note 29, at 2–3.

<sup>189</sup> *United States v. Cotterman*, 637 F.3d 1068, 1079, 1085 (9th Cir. 2011).

<sup>190</sup> See *Olmstead v. United States*, 277 U.S. 438, 466 (1928) (holding that the Fourth Amendment is not violated unless an official search or seizure has occurred).

<sup>191</sup> See Russell L. Weaver, *The Fourth Amendment, Privacy and Advancing Technology*, 80 Miss. L.J. 1131, 1150 (2010) [hereinafter *James Otis Lecture*] ("While the concepts of 'trespassory invasions' and 'intrusions into constitutionally protected areas' may have made sense as applied to a house, a car, or a briefcase, those concepts did not produce satisfactory results as advancing technology provided police investigators with ever more sophisticated surveillance technologies.").

<sup>192</sup> *Id.* at 1138.

<sup>193</sup> *Id.*

that such technologies would allow governmental officials to spy on citizens without actually entering their homes or touching their persons.<sup>194</sup>

Because of the context in which the Fourth Amendment developed, the U.S. Supreme Court originally defined the term “search” in a narrow way that focused only on the historical abuses that concerned the Framers.<sup>195</sup> The Framers were familiar with actual physical searches by British officials of persons, houses, papers, and effects; thus, the Court tended to define the term “search” by reference to actual physical searches of areas or persons and frequently inquired whether governmental officials had intruded or trespassed into a “constitutionally protected area.”<sup>196</sup> If the police broke into someone’s house (or, for that matter, an automobile), and thoroughly searched it, the courts concluded that the police had intruded upon a constitutionally protected area and therefore had committed a search within the meaning of the Fourth Amendment.<sup>197</sup>

By the twentieth century, although advances in police surveillance technology had begun to present significant challenges to the Court’s historical definition of the term search, the Court continued to focus on whether police or governmental officials had intruded or trespassed into constitutionally protected areas.<sup>198</sup> However, the Justices began to actively debate whether the Court should continue to follow its historical approach or whether advances in technology suggested the need for a new and different approach.<sup>199</sup>

Early in the twentieth century, the Court was confronted by several different types of cases that involved advancing technology.<sup>200</sup> In general, although a number of Justices were beginning to dissent,<sup>201</sup> the Court continued to adhere to the idea that a “search” required a “trespass” into a “constitutionally protected area.”<sup>202</sup> In its landmark decision in *Katz v. United States*,<sup>203</sup> the Court articulated a different approach

<sup>194</sup> See *id.* at 1133.

<sup>195</sup> See, e.g., *Carroll v. United States*, 267 U.S. 132, 147, 149 (1925); *Hester v. United States*, 265 U.S. 57, 59 (1924) (concluding that “the special protection accorded by the Fourth Amendment to the people in their ‘persons, houses, papers, and effects,’ is not extended to the open fields”).

<sup>196</sup> See, e.g., *Lopez v. United States*, 373 U.S. 427, 438–39 (1963); *Silverman v. United States*, 365 U.S. 505, 510–12 (1961).

<sup>197</sup> See, e.g., *Carroll*, 267 U.S. at 153–54, 156.

<sup>198</sup> See Weaver, *James Otis Lecture*, *supra* note 191, at 1139.

<sup>199</sup> See *id.*

<sup>200</sup> See, e.g., *Silverman*, 365 U.S. at 506–07 (involving use of a “spike mike” that was inserted into defendant’s home and allowed police to overhear conversations occurring inside the home); *Goldman v. United States*, 316 U.S. 129, 131–32 (1942) (involving use of a “detectaphone” that allowed the police to overhear conversations that occurred in an adjoining office); *Olmstead v. United States*, 277 U.S. 438, 456–57 (1928) (involving wiretapping devices placed outside defendants’ homes and businesses).

<sup>201</sup> See Weaver, *James Otis Lecture*, *supra* note 191, at 1150.

<sup>202</sup> See *id.* at 1139.

<sup>203</sup> 389 U.S. 347 (1967).

for evaluating whether a search occurs. In that case, the Court focused on whether governmental officials had violated Katz's expectation of privacy.<sup>204</sup> In doing so, the Court shifted its Fourth Amendment focus from places to persons<sup>205</sup> and inquired whether the police had violated Katz's "expectation of privacy." The Court stated: "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."<sup>206</sup> Justice Harlan, concurring, agreed with the Court that the focus should be on whether Katz had an expectation of privacy (EOP), but he argued that the expectation must be one that society was prepared to recognize as reasonable.<sup>207</sup> Ultimately, Harlan's requirement of "reasonableness" was integrated into the EOP test, such that the Court inquired whether the police had intruded upon an individual's "reasonable expectation of privacy" (REOP).<sup>208</sup> The trespass test did not entirely disappear.<sup>209</sup>

Under the *Katz* approach, there is a legitimate question about whether governmental officials conduct a "search" within the meaning of the Fourth Amendment when they intercept electronic communications that traverse international borders.<sup>210</sup> An ordinary person might readily conclude that the government performs a "search" when it examines the content of his or her electronic communications. Many people assume that their electronic communications are private—at least against governmental prying. However, the cases mentioned earlier (suggesting that one has no REOP at the nation's borders) suggest otherwise. Moreover, in a number of cases, the Court has held that individuals do not retain an REOP in information that they voluntarily turn over to third parties.<sup>211</sup> Since electronic communications usually go through multiple third parties, and the sender "voluntarily" turns those communications over to those third

---

<sup>204</sup> *Id.* at 351–52.

<sup>205</sup> *Id.* at 351 ("For the Fourth Amendment protects people, not places.").

<sup>206</sup> *Id.* at 351–52 (citations omitted).

<sup>207</sup> *Id.* at 361 (Harlan, J., concurring) ("As the Court's opinion states, 'the Fourth Amendment protects people, not places.' The question, however, is what protection it affords to those people. Generally, as here, the answer to that question requires reference to a 'place.' My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'").

<sup>208</sup> *See, e.g.,* *United States v. Jones*, 132 S. Ct. 945, 950 (2012).

<sup>209</sup> *See id.* at 947 ("*Katz* did not repudiate the understanding that the Fourth Amendment embodies a particular concern for government trespass upon the areas it enumerates.").

<sup>210</sup> *See Weaver, James Otis Lecture, supra* note 191, at 1193–95.

<sup>211</sup> *See, e.g.,* *Smith v. Maryland*, 442 U.S. 735 (1979) (holding that police use of a pen register to record the phone numbers called by an individual did not constitute a search); *United States v. Miller*, 425 U.S. 435 (1976) (holding that there was no search where the government seized checks and other bank records that defendant had turned over to a bank); *Couch v. United States*, 409 U.S. 322 (1973) (holding that there was no search where the government seized books and other documents from an accountant to which defendant had delivered them).

parties, legitimate questions might be raised about whether they are accompanied by an REOP so that governmental examination of electronic communications constitutes a “search” within the meaning of the Fourth Amendment. On the bright side, for those who believe that the government’s seizure of electronic communications should be regarded as searches, *Katz* held that the police committed a “search” when they used a listening device to overhear a conversation that took place over a public phone and therefore was sent through a third party (the phone company) to a third party (the recipient of the phone call).<sup>212</sup> However, *Katz* has provided limited protection in subsequent decisions.<sup>213</sup>

Even if the government’s review of electronic communications constitutes a search within the meaning of the Fourth Amendment, it is not at all clear that the Court would require a warrant or probable cause for those searches. Case law from earlier periods suggests that the government has the power to open and read letters and other documents that cross the borders of the United States. For example, in *United States v. Ramsey*,<sup>214</sup> a U.S. customs inspector opened incoming first class international mail without a warrant, and also intercepted international phone calls.<sup>215</sup> Although the applicable administrative regulations permitted customs officials to search international mail whenever they had “reasonable cause” to believe that the mail contained items prohibited under U.S. law, the D.C. Court of Appeals invalidated the search on the basis that it was conducted without a warrant or probable cause.<sup>216</sup> As a result, *Ramsey* directly addressed the question of whether the government had the power to review communications that crossed international borders.<sup>217</sup> In doing so, the Court recognized broad

---

<sup>212</sup> The Government stresses the fact that the telephone booth from which the petitioner made his calls was constructed partly of glass, so that he was as visible after he entered it as he would have been if he had remained outside. But what he sought to exclude when he entered the booth was not the intruding eye—it was the uninvited ear. He did not shed his right to do so simply because he made his calls from a place where he might be seen. No less than an individual in a business office, in a friend’s apartment, or in a taxicab, a person in a telephone booth may rely upon the protection of the Fourth Amendment. One who occupies it, 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. To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.

*Katz*, 389 U.S. at 352.

<sup>213</sup> See Weaver, *James Otis Lecture*, *supra* note 191, at 1158–59.

<sup>214</sup> 431 U.S. 606 (1977).

<sup>215</sup> *Id.* at 608–10.

<sup>216</sup> *Id.* at 611.

<sup>217</sup> *Id.* at 619–20 (“Respondents urge upon us, however, the position that mailed letters are somehow different, and, whatever may be the normal rule with respect to border searches, different considerations, requiring the full panoply of Fourth Amendment protections, apply to international mail.”).

authority on the part of the U.S. government to conduct border searches: “[S]earches made at the border, pursuant to the long-standing right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border, should, by now, require no extended demonstration.”<sup>218</sup> The Court went on to further emphasize the scope of federal power:

This acknowledgment of plenary customs power was differentiated from the more limited power to enter and search “any particular dwelling—house, store, building, or other place” where a warrant upon “cause to suspect” was required. The historical importance of the enactment of this customs statute by the same Congress which proposed the Fourth Amendment is, we think, manifest.<sup>219</sup>

In *Ramsey*, the Court indicated that the breadth of federal authority at the nation’s borders “has been faithfully adhered to” by the Court.<sup>220</sup>

In the Court’s view, the government had the right to examine letters and other correspondence that crossed the nation’s borders.<sup>221</sup> It mattered not whether the letters were being carried across the border by an individual, or whether they had been sent through the U.S. mail:

It is clear that there is nothing in the rationale behind the border-search exception which suggests that the mode of entry will be critical. It was conceded at oral argument that customs officials could search, without probable cause and without a warrant, envelopes carried by an entering traveler, whether in his luggage or on his person. Surely no different constitutional standard should apply simply because the envelopes were mailed, not carried. The critical fact is that the envelopes cross the border and enter this country, not that they are brought in by one mode of transportation rather than another. It is their entry into this country from without it that makes a resulting search “reasonable.”<sup>222</sup>

Justice Stevens, joined by two other Justices, challenged the Court’s interpretation of the Fourth Amendment, citing the historic respect accorded by the Court to the private

---

<sup>218</sup> *Id.* at 616.

<sup>219</sup> *Id.* at 616–17.

<sup>220</sup> *Id.* at 617.

<sup>221</sup> *See id.* at 621–22.

<sup>222</sup> *Id.* at 620 (citation omitted).

communications of individuals.<sup>223</sup> He noted, “[i]f the Government is allowed to exercise the power it claims, the door will be open to the wholesale, secret examination of all incoming international letter mail. No notice would be necessary either before or after the search.”<sup>224</sup>

In a similar vein, in *United States v. Seljan*,<sup>225</sup> customs inspectors opened a sealed envelope containing personal correspondence. Since the search took place at the nation’s borders, the Court held that the search was valid under the Fourth Amendment.<sup>226</sup>

#### CONCLUSION

The administrative exception to the warrant requirement is well-recognized, and has led to a variety of administratively related doctrines and offshoots. Under that exception, the Court has altered the Fourth Amendment’s probable cause and particularity requirements, dispensed with the requirement of a warrant for some administrative searches, and provided the government with broad powers to search at the nation’s international borders.

It is not clear that the Framers of the Fourth Amendment really intended for administrative inspections to be treated differently than other inspections or searches.<sup>227</sup> Following the British colonial period, the new American colonists were incensed regarding the use of writs of assistance and general warrants by British colonial officials, and these writs and warrants had frequently been used in administrative contexts.<sup>228</sup> In particular, they had been used by customs officials.<sup>229</sup> As a result, it is not clear that historical considerations justify a line of demarcation between administrative inspections and other searches.

If the special (and reduced) status accorded to administrative searches ever did make sense, it continues to make sense in a modern technologically driven society. As technology has changed, the administrative exception has potentially far-reaching consequences for individual privacy. This is especially true for the border exception. The broad scope of governmental authority provided by this exception might have made sense in earlier times. No one disputes the notion that the U.S. government has the right to make sure that those who seek to enter the United States have the right to enter, and that they are not carrying contraband. As a result, the U.S. Supreme Court has always given the United States broad powers to conduct border searches. However, it is not

---

<sup>223</sup> *Id.* at 626 (Stevens, J., dissenting) (“The notion that private letters could be opened and inspected without notice to the sender or the addressee is abhorrent to the tradition of privacy and freedom to communicate protected by the Bill of Rights.”).

<sup>224</sup> *Id.* at 632.

<sup>225</sup> 547 F.3d 993 (9th Cir. 2008).

<sup>226</sup> *Id.* at 1011.

<sup>227</sup> See Weaver, *James Otis Lecture*, *supra* note 191, at 1138, 1140, 1176.

<sup>228</sup> *Id.* at 1138.

<sup>229</sup> *Id.* at 1131–33 & nn.4 & 6.

clear that the government's right to conduct border searches can or should give the government the right to search (or retain or copy) computers and electronic devices at the nation's borders, or the right to intercept international electronic searches. Computers (including iPhones, thumb drives, etc.) can store large amounts of information, including much personal information. Indeed, given that some computers are programmed to connect to cloud storage sites, the government's ability to access a personal computer can give the government access to virtually all of the "papers" and "documents" in an individual's life. At least some of this information will be personal and confidential, and border officials should not be allowed to routinely search computers, iPhones, and other electronic devices.

As the courts grapple with these issues, they will be forced to determine the standard to be applied to detailed searches of electronic devices. The court of appeals' decision in *Cotterman* suggests that customs officials should be allowed to make routine and cursory searches of electronic files without cause, but they should be required to show "reasonable suspicion" in order to conduct a more detailed forensic examination.<sup>230</sup> Whether the "reasonable suspicion" standard provides enough protection against a computer search is debatable. In *Cotterman*, an individual's computer was seized, sent to a distant place, and held for several days.<sup>231</sup> One can argue that such an "intrusion" on individual privacy should require a warrant based on probable cause. Undoubtedly, the government's decision to seize and hold someone's computer can have important personal and business consequences for that individual.

---

<sup>230</sup> See *United States v. Cotterman*, 709 F.3d 952, 968 (9th Cir. 2013).

<sup>231</sup> *Id.* at 956.