

2018

## The forensic Digital Search of Cell phones at the Border in the United States v. Kolsuz: Tough on Terrorism or Tough on Petty Crime?

Jillian Bates

Follow this and additional works at: <https://archives.law.nccu.edu/ncclr>



Part of the [International Law Commons](#)

---

### Recommended Citation

Bates, Jillian (2018) "The forensic Digital Search of Cell phones at the Border in the United States v. Kolsuz: Tough on Terrorism or Tough on Petty Crime?," *North Carolina Central Law Review*. Vol. 41 : No. 1 , Article 4.

Available at: <https://archives.law.nccu.edu/ncclr/vol41/iss1/4>

This Article is brought to you for free and open access by History and Scholarship Digital Archives. It has been accepted for inclusion in North Carolina Central Law Review by an authorized editor of History and Scholarship Digital Archives. For more information, please contact [nperry@nccu.edu](mailto:nperry@nccu.edu).

## **THE FORENSIC DIGITAL SEARCH OF CELL PHONES AT THE BORDER IN *UNITED STATES V. KOLSUZ*: TOUGH ON TERRORISM OR TOUGH ON PETTY CRIME?**

BY: JILLIAN A. BATES

### INTRODUCTION

Modern cell phones are no longer just communication devices. For many, they are extensions of their daily lives. Modern cell phones have the capability to “learn” the particulars of its user, including the places the user regularly visits, the user’s political leanings, and details of the user’s social, familial, and professional life. Today, intimate details of a person’s private life are stored on a cell phone. Specific functions and social expectations have been created to protect this private information. It is a commonly accepted social standard that scrolling through the content of another’s cell phone without permission constitutes an invasion of privacy. However, this same privacy does not apply to the government as long as the person is walking through customs before or after an international flight. According to a ruling issued by the Fourth Circuit Court of Appeals in 2018, government agents at international airports have the right to confiscate a person’s cell phone and conduct a forensic digital search of all the data stored on the person’s cell phone as long as they have a reason to suspect that a crime may have been committed.<sup>1</sup> In short, passcodes and social norms cannot withstand the reach of the United States government as long as government agents reasonably suspect the person of committing a crime. In this note, I will address the Fourth Circuit’s failure to consider limitations on the scope of the forensic search of individual’s cell phones as it relates to minor crimes at international airports, in *United States v. Kolsuz*. I will also address the implications of such intrusive searches as they relate to government overreach in the policing of minor crimes as well as the vulnerable communities that will most likely be disproportionately affected by these intrusive searches.

---

1. *United States v. Kolsuz*, 890 F.3d 133, 146-47 (4th Cir. 2018), as amended (May 18, 2018).

## THE CASE

In December 2012, Hamza Kolsuz arrived at John F. Kennedy International Airport (JFK) in New York for a flight to Turkey.<sup>2</sup> At check in, customs agents discovered 163 firearms parts, listed on the United States Munitions List (USML), in his luggage.<sup>3</sup> Agents explained to Kolsuz that he was required to have a specific export license in order to carry the items onto his international flight, and subsequently seized the weapons parts.<sup>4</sup> In January 2013, Kolsuz, again, attempted to carry weapons parts listed on the USML on an international flight from JFK to Turkey without the requisite export license.<sup>5</sup> As a consequence, the weapons were seized.<sup>6</sup> On February 1, 2016, a Special Agent with United States Customs and Border Protection (CBP) in New York discovered that Kolsuz had again entered the country and had an upcoming flight from Washington Dulles International Airport (Dulles) to Turkey.<sup>7</sup> The CBP Officer proceeded to inform other CBP officers at Dulles of Kolsuz's flight as well as his history of attempting to smuggle weapons parts out of the country illegally.<sup>8</sup> Upon Kolsuz's arrival at Dulles, CBP officers searched his checked bags and found multiple firearms parts listed on the USML.<sup>9</sup> Before boarding his flight, Kolsuz was stopped and transported to a secondary inspection area.<sup>10</sup> There, the officers discovered that he had no active or pending export license and initiated two searches of his iPhone.<sup>11</sup> The first search was a manual search, where agents manually scrolled through his recent calls and text messages.<sup>12</sup> Following an interview with CBP officers Kolsuz was arrested.<sup>13</sup> The officers then transported Kolsuz's iPhone to a Homeland Security Investigation office and conducted a forensic search of his cell phone.<sup>14</sup> Data was extracted from the cell phone itself using a Cellebrite Physical Analyzer.<sup>15</sup> This process lasted for a month and resulted in a report including information regarding "Kolsuz's contact lists, emails, messenger conversations, photographs, videos, calendar, web browsing history," call logs, and GPS coordinates of

---

2. *Kolsuz*, 890 F.3d at 138-39.

3. *Id.*

4. *Id.*

5. *Id.*

6. *Id.*

7. *Id.* at 138-39.

8. *Id.*

9. *Id.*

10. *Id.*

11. *Id.*

12. *Kolsuz*, 890 F.3d at 138-39.

13. *Id.*

14. *Id.*

15. *Id.*

his past physical locations.<sup>16</sup> This information made up a 896-page report.<sup>17</sup> Ultimately, Kolsuz was indicted for attempting to export firearms parts on the USML without a license, attempting to smuggle goods from the United States, and conspiracy.<sup>18</sup>

Kolsuz made a pre-trial motion to suppress the report that was generated following the forensic search of his cell phone.<sup>19</sup> He contended that a month-long forensic search of his phone at a location situated miles away from the international airport following his arrest “should be treated as a search incident to his arrest,” rather than subject to the border search exception.<sup>20</sup> In addition, he contended that, under *Riley v. California*, “cell phones may be searched incident to an arrest only with a warrant based on probable cause.”<sup>21</sup> The district court denied Kolsuz’s motion to suppress and held that the search following his arrest constituted a border search, based on the finding that prior to the forensic search, neither made that search incidental to his arrest nor rendered the border exception inapplicable.<sup>22</sup> Moreover, the court held that a search that is initiated at the border is subject to the border exception regardless of whether it was conducted off-site and for a long period of time.<sup>23</sup> Thus, the manual search of Kolsuz’s iPhone was a routine border search, requiring no warrant; and the off-site forensic search of Kolsuz’s iPhone was a nonroutine border search, which required only reasonable suspicion.<sup>24</sup> Ultimately, the court rejected the finding in *Riley*.<sup>25</sup> Kolsuz appealed the district court’s finding to the United States Court of Appeals for the Fourth Circuit.<sup>26</sup> This court affirmed the district court’s decision, and held that the forensic search of Kolsuz’s phone, and the subsequent invasion of Kolsuz’s privacy, was justified under the border search exception because there was sufficient evidence for the officers to establish reasonable suspicion that Kolsuz was actively engaging in an ongoing crime and possible conspiracy.<sup>27</sup>

---

16. *Id.*

17. *Id.* at 138-39.

18. *Id.*

19. *Id.*

20. *Id.* at 140.

21. *Id.*

22. 890 F.3d at 140.

23. *Id.*

24. *Id.*

25. *Id.*

26. *Id.*

27. *Id.* at 148.

## BACKGROUND

The Fourth Amendment provides individuals with the right “to be secure in their persons, houses, paper, and effects against unreasonable searches and seizures” absent a warrant and probable cause.<sup>28</sup> However, border searches are an exception to this requirement.<sup>29</sup> The border search exception applies during an individual’s entrance and exit of the country by way of an international border or its “functional equivalent,” such as an international airport.<sup>30</sup> There are two types of border searches, routine and nonroutine.<sup>31</sup> During a routine border search “government agents may conduct searches of individuals’ person or property absent any warrant or level of individual suspicion.”<sup>32</sup> Routine searches of electronic devices, such as cell phones, involve a “manual inspection,” where government agents may assess the contents of an individual’s cell phone “in the same manner as a typical user.”<sup>33</sup> This includes using the phone’s touch screen function to view stored text messages and phone calls.<sup>34</sup> A nonroutine border search is more intrusive than a routine search.<sup>35</sup> In *United States v. Saboonchi*, the Fourth Circuit held that the digital forensic search of a cell phone is a non-routine search.<sup>36</sup> A forensic digital search is typically where officers conduct a detailed review of the data stored in an individual’s cellular device using a special process.<sup>37</sup> Courts have referred to these digital forensic searches as body cavity searches of an electronic device.<sup>38</sup> In order to perform a nonroutine border search, government agents are required to first have reasonable or individualized suspicion.<sup>39</sup> This means that agents must have “a particularized and objective basis for suspecting the particular person stopped of criminal activity.”<sup>40</sup> This reasonable suspicion standard was questioned in *Riley v. California*.<sup>41</sup> In that case, the court held that, due to modern cell phones’ immense storage capacity, the search of a person’s cell phone following their arrest should be

---

28. U.S. Const. amend. IV.

29. *United States v. Kolsuz*, 185 F. Supp. 3d 843, 850-51 (E.D. Va. 2016), *aff’d*, 890 F.3d 133 (4th Cir. 2018), *as amended* (May 18, 2018).

30. *Id.*

31. *Id.*

32. *Id.* at 852.

33. *Id.* at 854. (citing *United States v. Ickes*, 393 F.3d 501 (4th Cir.2005)).

34. 185 F. Supp. 33d at 854.

35. *Id.* at 853.

36. *Id.* at 854. (citing *United States v. Saboonchi*, 990 F.Supp.2d 536, 569 (D.Md.2014)).

37. 185 F. Supp. 33d at 854.

38. *Id.* at 854. (citing *United States v. Saboonchi*, 990 F. Supp.2d 536, 560 (D. Md. 2014)).

39. 185 F. Supp. 33d at 854.

40. *Id.* at 859. (citing *United States v. Cortez*, 449 U.S. 411, 417-18, 101 S. Ct. 690, 66 L. Ed. 2d 621 (1981)).

41. *Riley v. California*, 134 S. Ct. 2473, 189 L. Ed. 2d 430 (2014).

subject to a warrant and probable cause, as provided by the Fourth Amendment.<sup>42</sup>

## ANALYSIS

The purpose of the border search exception to the Fourth Amendment is to allow the government's interest in national security, transnational security, and export control to govern at its international border.<sup>43</sup> It is appropriate that the government have strict rules and absolute power over international borders. The government has every right to protect its interest at its borders, which include protecting its citizens from terrorist attacks like those on September 11, and the Orlando nightclub shooting. However, when government agents at the border are faced with arguably minor, petty crimes, is it reasonable to use expensive resources to violate individuals' privacy with the limitless and intrusive forensic data search of a suspect's cell phone? In *Kolsuz*, the court failed to address whether searches should be more narrowly tailored when government agents are confronted with individuals who may have committed minor crimes at international airports.<sup>44</sup> The limitless forensic search of a person's cell phone is only justifiable, under the purpose of the border search exception, when it is used to prevent real threats of major crimes, such as threats of terrorism, and conspiracies to flood countries with dangerous drugs, firearms or other illegal contraband, like in *Kolsuz*. On a smaller scale, the forensic data search of an individual's cell phone is not a justifiable approach to securing international borders. Instead, these unfettered forensic searches of cellular devices at the border subject individuals' unrelated personal information to overexposure; and also subject commonly marginalized groups that regularly face racial and religious profiling to a greater likelihood of violations of their privacy rights while at international airports.

### I. THE OVEREXPOSURE OF UNRELATED PERSONAL INFORMATION.

Although, nonroutine border searches are exceptions to the Fourth Amendment right to be free from unreasonable searches and seizures absent a warrant, the exception should be subject to certain limitations based on the nature of the alleged crime. In the event that government agents at

---

42. *Kolsuz*, 185 F. Supp. 3d at 851. (citing *Riley v. California*, 134 S. Ct. 2473, 189 L. Ed. 2d 430 (2014)).

43. *Kolsuz*, 890 F.3d at 143-44.

44. *Id.* at 150 (Wilkinson, J., concurring) ("We have no idea the dangers we are courting. Thousands of travelers go through [border posts] every day. Yet the majority hardly grapples with how law enforcement is expected to ascertain individualized suspicion when dealing with such numbers.").

international airports find it reasonable to suspect a person of committing a minor crime, such as stowing a small amount of weed in their luggage prior to their flight abroad, there should be specific limitations on how extensive a forensic data search of their phone, if one is conducted, is permitted to be. In *Kolsuz*, the court did not consider the possibility of a forensic data search of a person's cell phone after they had been suspected of committing a minor crime.<sup>45</sup> Instead, it only considered forensic data searches as they applied to major crimes that involved export control and possible security interests abroad.<sup>46</sup> The court's failure to distinguish between the treatment of major and minor crimes permits the potential for a deeply intrusive level of search that may not be warranted depending upon the crime suspected.

Moreover, this has the potential to subject an individual to a search that may easily stray from the original purpose or go beyond the border search exception. In short, the search may become analogous to a fishing expedition. As a result, the data stored in the cell phone of a suspect, who may be a doctor, lawyer, or a fiduciary, may be that of another party. In turn, the search and seizure of those documents may violate the third party's Fourth Amendment rights, which were not originally subject to the border search exception, or violate the third party's privacy over those records that are legally protected in their own right for the best interest of a third party patient or client.

## II. THE OVEREXPOSURE OF REGULARLY PROFILED GROUPS TO INTRUSIVE SEARCHES.

This gap in the law also allows room for vulnerable groups of people who are regularly profiled as violent or criminals in the United States to be more likely to have their cell phone's subject to a forensic search at the border. Due to past and recent instances of terrorism, both domestically and abroad, the security at airports has become increasingly stricter. Much of the time, these terrorist attacks have been orchestrated by religious extremist or their sympathizers, who have commonly and unfairly been associated with people of the Islamic faith as well as people of Middle Eastern descent. As a consequence, innocent Muslims and people of Middle Eastern descent have been stigmatized as terrorists or terrorist sympathizers and routinely face racial or religious profiling, particularly at airports. In addition to the latter mentioned groups, in the United States, people of color and immigrants also face racial profiling as well as frequent suspicion of involvement in criminal activity. These groups, which are already vulnerable to racial and religious

---

45. *Id.*

46. *Id.* at 143 (majority opinion) (court focused on the transnational offense).

profiling as well as unfair association with minor crimes, will likely be the demographics most frequently having their cell phones subjected to intrusive forensic data searches at airports over suspicion of petty crime. Although, officers are required to first satisfy the reasonable suspicion standard before proceeding with a forensic search, there is evidence of many instances where these marginalized groups have been singled out and assumed to be violent or taking part in illegal activity based on their phenotype or obvious religious associations, regardless of this standard. A couple of instances include, but are not limited to, the senseless killings of people of color such as Philando Castile, and President Donald Trump's so-called "Muslim Ban". These groups' cell phones will likely be subject to limitless searches as a result of government agent's suspicion of their involvement in minor crimes at international airports. Ultimately, the *Kolsuz* court's failure to mention any distinction between the extent of a forensic search in the case of the suspicion of a minor crime versus a major crime leaves room for needlessly extensive violations of privacy as well as prejudice.

#### CONCLUSION

Although the border search exception to the Fourth Amendment is beneficial in that it secures the United States border for reasons of national security and export control, it lacks specificity regarding the suspicion of minor crimes. This allows for the overexposure of unrelated personal information via intrusive forensic searches of individuals' cell phones, and the disproportionate subjection of vulnerable and marginalized groups in the United States to these searches as well as additional discriminatory treatment and more frequent exclusion from the privacy protection as promised under the Fourth Amendment while at international airports. Exceptions without reasonable limitations are dangerous, especially when the exception includes governmental overreach into the immensely private lives of already vulnerable demographics.