Research Paper on US Border Privacy

Feliz Nunez

[Institutional Affiliation(s)]

Author Note

Research Paper on US Border Privacy

The attacks of September 11th made U.S. airports and airliner security a major priority, and led to increased border security. It led to heavy investments to enhance security measures over the previous decades, which included stricter screening procedures for baggage and procedures, x-ray screenings, metal detectors, explosives screenings and more recently smartphone and laptop checks. However, the increased screening and security measures have been labeled as improper, overly intrusive and humiliating, that threatens the privacy and thus civil liberties of passengers and entrants, even that of U.S. citizens. The paper will examine these claims and discuss US Border Security measures in light of privacy concerns and violations of civil liberties.

The grievance of the American public over compromised privacy as a result of border screenings was seen when nearly 250 people complained that U.S. border security officials searched their phones and laptops, containing private content, without a warrant (Savage & Nixon, 2017). However, government agents have since long been allowed to examine possessions of entrants without requiring a warrant or a ‘reasonable basis’. However, personal electronic items and smartphones often contain private information which is not at the same level as luggage, which leads to a significantly high sense of privacy violation. Screenings usually involve agents searching through the citizens’ devices and private data either in front of them, or sending in the device for a forensic search that will involve copying all the data for a deeper examination into the contents.

The threats to privacy have recently led to a number of litigations in which rights lawyers claim that random screenings and searches violate Fourth Amendment rights. A number of people belonging to different backgrounds, professions have filed claims against the US Government, in particular people belonging to the Muslim faith. The rising number of claims correlate with a reported increase in the number of searches that have risen nearly 60% over the last two years (Canadian Press, 2018). For Border security officials and Homeland Security, the screenings are justified on the pretext of combatting child pornography and terrorism.

The ‘U.S. Customs and Border Protection’ upon mounting rulings and complains issued new directives to their border agents and established regulations in which new limits were placed on accessing phones of travelers, demanding passwords, copying files, conducting searches and on accessing stored items in the cloud. Nevertheless, agents are still allowed to demand a password to unlock electronic devices without requiring a probable cause to do so. Although, new regulations allow travelers to refuse, but a refusal can often lead to further consequences and complications. Moreover, agents are allowed only to search apparent data and not access older items inside cloud storage. Furthermore, border agents are not allowed to prevent citizens from entering the country despite their refusal to provide access to their devices. A refusal, however, may lead them to ask more intrusive questions, carry out extensive searches, increase detention length or refer the traveler to a more advanced search. In case, there is a national security concern; agents are authorized to connect the device to a hard drive, copy its contents and retain the data if there exists a probable cause or a security concern. Otherwise, they are instructed to destroy the data and return the electronic devices to the owner. Detaining devices require them to sign a form and obtain management approval if detention is to be prolonged (Canadian Press, 2018).

The wide scope of inspection powers given to U.S. border officials has also been a concern for other nations, in particular, Canada owing to the extensive cross border movement that takes place. Canadian authorities, for instance, warn their citizens that traveling to the U.S. may require them to provide passwords to their electronic devices, and that searches do not require pre-existing evidence or warrants. Whether they are U.S. citizens who travel to Canada and are returning back, or Canadian citizens, anyone can be subject to a routine border inspection that involves mobile device screenings, without grounds. Furthermore, they are also alerted to the possibility that advance searches require a genuine national security concern or reasonable suspicion of involvement in illegal activities, and in this regard, their powers may vary from that of Canada, EU or the UK (OPC, 2018). Any restrictions on the searches such as accessing apparent data and not accessing cloud storage are also advised to citizens along with precautionary measures in order to avoid complications.

The unusually high powers afforded to border security have also been challenged by civil liberty unions, groups, and activists who have frequently expressed concern about the growing practice of mobile phone and electronic device screenings. The key cause of concern is that these powers allow officials to unlock the devices and scan through social media accounts, text messages, private photos, and legal information. There is also reason for concern whether similar practices would be implemented in case of domestic travelers within the U.S. which could, in turn, lead to greater apprehensions about privacy violations and increasing government surveillance. The issue of privacy is growingly recognized as a social and individual value internationally by the OECD, the UN or the ECJ. Its recognition as a universal human right has influenced legislation concerning data protection, bioethics, copyright protection as well as security (Löfgren, Strange, & Backman, 2013). As the threat of global terrorism became serious, there was a surge in security measures and technology globally that have frequently involved some form of privacy intrusion. Consequently, that led to disagreement and debate over privacy considerations against demands for stricter security. Rights groups express fears of the U.S. slowly turning into a ‘surveillance society' in which privacy infringement and surveillance becomes socially acceptable.

The United States in comparison to other western countries face a range of challenges in the issue of privacy. The right to privacy is not as explicit in the United States Constitution; however, the Supreme Court has developed rulings based on the First and the Fourth Amendment, and the U.S. Bill of Rights. Thus, certain guarantees and limitation were developed and defined by the Supreme Court in a decision such as *Katz v United States*. One of the principles established in these cases was that a voluntary handing over of personal data to a 3rd party implies a relinquishment of the right to privacy for an individual against the state. The U.S. Supreme court litigation, however, remains limited in its rights-based approach and has so far worked to provide protection exclusive to U.S. citizens (Lachmayer, 2015). Data privacy protection and associated frameworks fall within the domain of the legislature rather than the constitution. And thus, an enhanced focus on counter-terrorism by the U.S. Congress has led to the promotion of security measures rather than privacy concerns. As a result intelligence and security agencies were able to access personal data more easily. The priorities of the Congress towards counter-terrorism encouraged the administration to implement state surveillance measures (Lachmayer, 2015). However, with sweeping powers, further developments such as the Freedom Act demonstrate that there is a certain shift of concern, and efforts to limit surveillance and activities of intelligence agencies are underway.

In the U.S., the respect for civil liberties is an integral value that has been well defined and ingrained into legislation. At the same time, the Department of Homeland Security while expected to maintain security, is also expected to demonstrate an awareness of the sanctity of individual rights. It is therefore that all actions and strategies that Homeland Security formulates to enhance the nation’s security have to consider civil liberties simultaneously. The assertion that a compromise on civil liberties and rights is necessary to increase security suggests that these two important principles are in clash with each other. An acceptance of such a notion on the national level would condition the people to accept that civil liberties can be compromised at the cost of national or domestic security (Sutherland, 2014). This notion is problematic in of itself, and encourages government agencies, such as border security, to overlook privacy concerns.

Although the U.S. Constitution places clear limits on the ability of the government to search private properties of individuals without due right, the same limits are practically and legally, not as strong when it comes to the border. Many legal protections remain weak and prone to be overridden. Consequently, border agents hold an inherent view that they are permitted to infringe on a person’s private data stored in his or her electronic device on the slightest pretext. It is this understanding which gives them the sense of liberty to scrutinize any content stored on a person's laptop, phone or portable device, which includes a person's legal consultation, e-commerce activity, social media postings or any other forms of communication. These approaches have resulted into invasive and often abusive practices that have led to severe consequences in the case of some travelers, often times on small mistakes or errors they may have made (Cope, Kalia, Schoen, & Schwartz, 2017). It is, therefore, necessary to formulate better legal protections to help people having their rights infringed upon at the U.S. borders and to regulate and limit the scope of powers allocated to Border Security.

Moreover, the U.S. lags behind the EU and the UK when it comes to data privacy and protection from state surveillance and security agencies. A key difference lies in the legislature based approach the U.S. takes in this regard from the constitutional approach taken by the EU. Without constitutional protection, limitation of powers under counter-terrorism is a difficult and complex task, especially when state legislatures can differ with one another over the choice of having a privacy-friendly approach against security and surveillance based approach. A number of challenges exist both on the federal and the state level. Globally, there is an increasing demand to see data privacy to be recognized as a fundamental human right while at the same time governments strategize their counter-terrorism initiatives.

To conclude, the solution lies in battling crime, child pornography and terrorism in the ‘right’ way in order for the U.S. and its people and infrastructure to remain protected. A constructive national dialogue is required that embodies the principles of democracy and liberty while enacting legislation, and in the distribution of power. It is critical that civil rights groups advocate for better legislation to improve and protect digital privacy, as currently, the rights U.S. citizens have are fewer than they have near the U.S. border. Moreover, it is equally important that immigrants to the U.S. are provided similar protections. Stronger digital privacy protections are critical in the era where smartphones and electronic devices become more integrated into our daily lives and often contain sensitive private content. Although border security remains important in ensuring U.S. domestic security, the approach that border security has to clash with established rights to privacy must be challenged in order to develop a future where protecting privacy, and civil liberties remain a priority.

# References

Canadian Press. (2018, January 18). *U.S. border guards can search your phone: here are some details on how*. Retrieved January 7, 2019, from CBC: https://www.cbc.ca/news/technology/usa-border-phones-search-1.4494371

Cope, S., Kalia, A., Schoen, S., & Schwartz, A. (2017). *Digital Privacy at the U.S. Border: Protecting the Data on Your Devices and In the cloud.* Electronic Frontier Foundation. Retrieved from https://thinkdifferent.thepeoplesclub.org/wp-content/uploads/2018/02/digital-privacy-border-2017-guide3.10.17.pdf

Lachmayer, K. (2015). Rethinking Privacy Beyond Borders. *Tilburg Law Review, 20*, pp. 78-102. doi:10.1163/22112596-02001008

Löfgren, K., Strange, M., & Backman, C. (2013). Introduction: Privacy and Surveillance Policy in a Comparative Perspective. *Journal of Contemporary European Research, 9*(1), 116-119. Retrieved from http://muep.mau.se/bitstream/handle/2043/15267/520-2509-1-PB.pdf;jsessionid=8FD76993E7C502DEFF5EBC5F87E03325?sequence=2

OPC. (2018, December 17). *Your privacy at airports and borders*. Retrieved January 7, 2019, from Office of the Privacy Commissioner of Canada: https://www.priv.gc.ca/en/privacy-topics/public-safety-and-law-enforcement/your-privacy-at-airports-and-borders/#toc2

Savage, C., & Nixon, R. (2017, December 22). *Privacy Complaints Mount Over Phone Searches at U.S. Border Since 2011*. Retrieved January 7, 2019, from The New York Times: https://www.nytimes.com/2017/12/22/us/politics/us-border-privacy-phone-searches.html

Sutherland, D. W. (2014). Homeland Security and Civil Liberties: Preserving America. *Notre Dame Journal of Law, Ethics & Public Policy, 19*(1), 289-308. Retrieved from https://scholarship.law.nd.edu/cgi/viewcontent.cgi?article=1202&context=ndjlepp