Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/CLSR

Computer Law & Security Review

South Africa's PNR regime: Privacy and data protection

Kailey Taplin

University of Ottawa, Canada

ARTICLE INFO

Keywords:
PNR
Passenger name record
South Africa
Security
Personal data
Privacy
Data

ABSTRACT

There has been an increase in the collection and use of Passenger Name Record (PNR) data for security purposes globally. Though academic analysis of this trend has remained focused largely on the North American and European context, the Government of South Africa has been using PNRs since 2014 for security purposes. South Africa was the first country on the African continent to implement such a regime and is one of only thirteen states internationally to link its Advanced Passenger Information (API) and PNR systems. While there has been little attention on South Africa's use of PNRs, an inquiry into the country's PNR practices reveals striking privacy concerns, including the potential permanent retention of PNR data and a failure of the state to fully disclose if, and under what conditions, PNR data can be shared with other states. While South Africa has implemented a PNR regime that is comparable to the highest international standards, the data protection requirements appear to be far less developed. In fact, South Africa's PNR regime remains enigmatic as all indications and mention of PNR are elusive and scattered across government publications. As such, this paper aims to provide an introduction into the elements of South African PNR use, including the implications as they relate to law, data protection, and privacy.

1. Introduction

Ambitious forms of risk management practices are a growing feature of airport security strategies internationally: the use of Passenger Name Records (PNRs) is one such measure. A comprehensive PNR regime facilitates the collection and analysis of data related to persons travelling by commercial air transport and allows for pre-emptive risk management of all passengers. The practice of collecting and analysing passenger data and processing it through algorithms as well as cross checking it with national and international databases has profound implications on the fundamental rights of individuals. In the case of South Africa, this may represent the collection, retention, and transfer of personal data for purposes beyond the reasonable risk of the existing threat of terrorism and crime. Accordingly, it is both the "desire to prevent terrorism and the importance of protecting human rights that makes this a matter of pressing concern" as it relates to PNR use in the South African context.[1]

The information that is contained in PNR records allows states to improve security, combat terrorism, and make effective threat assessments by assisting with illegal migration, identifying passengers known to be a threat, providing better clearance at borders, and allowing for better allocation of border resources.[2] South Africa became the first country on the

E-mail address: ktapl031@uottawa.ca

[1] Thomas Hammarberg, *Protecting the Right to Privacy in the Fight against Terrorism*, (Strasbourg, France: Council of Europe, Commissioner for Human Rights, 4 December 2008), 2, www.europeanrights.eu/getFile.php?name=public/atti/commissario_ing.mht.

[2] International Civil Aviation Organization (ICAO), "Advance Passenger Information (API) & Passenger Name Record

https://doi.org/10.1016/j.clsr.2020.105524

African continent to use PNRs for security measures, and is one of only thirteen states globally that have linked their Advanced Passenger Information (API) systems with their PNR systems.[3] In doing so, South Africa became part of an international movement toward increased civil aviation security, but one that has led to new challenges in balancing security, surveillance, and individual privacy. Unlike its counterparts in North America and Europe, the Government of South Africa has not been transparent about its use of PNR in that there is a lack of publicly available information on the country's PNR procedures and its protection of personal data.

The South African PNR regime was implemented for national security purposes; however, it is fraught with ambiguity and there are serious implications on privacy and the protection of personal data of all individuals, irrespective of citizenship. In South Africa, the collection of PNR data facilitates the increased surveillance of all individuals but unlike its counterparts in North America and Europe, this subject has not yet become a central component of contemporary debate regarding the privacy - security trade off. While the collection of PNR data was quietly implemented prior to the 2010 FIFA World Cup hosted by South Africa,[4] the 2014 amendments to the South African Immigration Act (2002) solidified the collection and use of PNRs in the country for security purposes.[5] Since its implementation, conversation about the privacy implications has been limited to the Government of South Africa publicly stating that the use of PNRs would not be a concern for individuals,[6] particularly in light of the protection provided to them by the 2013 Protection of Personal Information (POPI) Act.[7] An examination of the PNR practices in South Africa demonstrates that there is potential for serious misuse and mistreatment of PNR data because at this time, there are no clear restrictions with respect to the collection, storage, transfer, or retention of the personal data that is collected.

The South African case is of considerable importance because it represents the first PNR regime to emerge on the African continent.[8] As such, this paper seeks to provide a comprehensive overview of the country's PNR regime and to present a number of critical issues related to PNR use, notwithstanding that South African officials have stated that personal data will be protected. The paper will also provide a brief overview of PNRs followed by the specifics of the South African PNR regime and an inquiry into the relevant laws and international standards related to PNR use and data protection.

2. What is PNR?

The International Civil Aviation Organization (ICAO) explains that a PNR is data that is generated when an airline ticket is booked and used by public authorities for the purpose of border control.[9] The collection of PNR data is not new; much of the information that makes up a PNR was already being gathered and registered by commercial airlines and was originally created to facilitate and ease airline bookings.[10] A PNR in its contemporary use in the air transport industry is described as an umbrella term used to refer to the information that is recorded by airlines and authorized agents for tickets booked by or on behalf of a passenger; the information is willingly provided by the passenger[11] and contains all data related to the booking.[12] A PNR is created each time a flight reservation is made and it is not deleted even if a reservation is cancelled or a ticket purchase is not finalized.[13] This data is then stored on an airline's database and various actors have access to the information.[14] The use of PNR data for security purposes became commonplace and controversial among states following the American implementation of, and increased demand for, PNRs after the terrorist attacks on New York City on September 11, 2001. Simply stated, the collection of PNR data is not new; however, the use of PNR data in the name of security is.

According to the ICAO, PNR data contributes to customs and immigration functions and facilitates air passenger traffic. The basis for state use of PNR data is derived from Arti-

(PNR): The ICAO Perspective," *ICAO: Uniting Aviation*, March 23, 2015, https://www.icao.int/APAC/Meetings/2015%20FAL/2.Day1.1045-1115.ICAOPerspective.API_PNR.2015March16.pdf#search=passenger%20name%20records.

[3] Inside MRO, "There Is Still Hope for African Aviation," Aviation Week Network, July 29, 2017, http://aviationweek.com/mro/there-still-hope-african-aviation.

[4] InterVISTAS, "South Africa Department of Home Affairs Border Management Consulting Services." InterVISTAS. http://www.intervistas.com/project/south-africa-department-of-home-affairsborder-managementconsulting-services/.

[5] *Government Gazette* 37679, Immigration Act 2002 (2014 amendments). 26 May 2014 [South Africa], http://www.dha.gov.za/IMMIGRATION_ACT_2002_MAY2014.pdf.

[6] The South African government stated that the collection and protection of personal data under the Immigration Act (2002), newly amended in 2014, would not be a concern because of the proposed implementation of the Protection of Personal Information Bill. Cf. "Speech by Andre Gaum during the National Assembly debate on the Immigration Amendment Bill," ANC Parliamentary Caucus, March 22, 2011, https://www.ancparliament.org.za/content/speech-andre-gaum-during-national-assembly-debate-immigration-amendment-bill-0.

[7] *Government Gazette* 37067, Protection of Personal Information Act , No. 4 of 2013 [South Africa]: https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013protectionofpersonalinforcorrect.pdf.

[8] Inside MRO, "There Is Still Hope for African Aviation".

[9] ICAO. "Passenger Data Exchange The Basics." 2013. https://www.icao.int/MID/Documents/2013/FALSeminar/Passenger Data Exchange_The Basics.pdf.

[10] Rocco Bellanova and Denis Duez, "A Different View on the 'Making' of European Security: The EU Passenger Name Record System as a Socio-technical Assemblage," *European Foreign Affairs Review* 17, no. 2 (2012):114.

[11] International Civil Aviation Organization (ICAO), *Guidelines on Passenger Name Record (PNR) data*, ICAO Document no. 9944 (Montreal, QC: International Civil Aviation Organization, 2010), https://www.iata.org/contentassets/18a5fdb2dc144d619a8c10dc1472ae80/new_doc_9944_1st_edition_pnr.pdf.

[12] European Commission, "The Passenger Name Record (PNR): Frequently Asked Questions." European Commission: Press Releases, July 13, 2007, http://europa.eu/rapid/press-release_MEMO-07-294_en.htm.

[13] Edward Hasbrouck, "What's in a Passenger Name Record (PNR)?" The Practical Nomad, accessed March 15, 2018, https://hasbrouck.org/articles/PNR.html.

[14] ICAO, *PNR Guidelines*.

cle 22 of the Convention on Civil Aviation (1944), known as the Chicago Convention, which recognizes the necessity for states to manage airline passengers who pass through international borders. The Convention suggests that all member states adopt efficient measures to ensure security and avoid unnecessary delays at all points throughout the airport – from check-in to customs and immigration.[15] Further, Article 29 (f) of the Chicago Convention states that an airline must carry a document with "a list of [passengers'] names and places of embarkation and destination."[16] While the initial intention of the Chicago Convention was somewhat vague, it is being used increasingly to justify PNR use and politically motivated surveillance practices.

International surveillance mechanisms have three distinct uses of PNR data.[17] First, PNR data can be used reactively to investigate a crime that has already been committed.[18] Second, PNR data can be used in real time prior to a passenger's departure or arrival.[19] In this manner, officials can use PNR data to prevent crime and identify high-risk individuals based on their patterns of behaviour. Third, PNR data can be used proactively based on criteria for 'suspicious behaviour'.[20] Much of contemporary PNR use relies on technology that allows data to be processed on a large scale, automated basis on a platform that allows the data to be shared among many national and international actors and agencies. The result is that PNR data is now a valuable tool for states to provide aviation security by producing accurate threat assessments of passengers. To this end, the "critical value of PNR data has prompted some states to enact legislation or develop draft legislation for approval by their Legislatures requiring that aircraft operators provide their public authorities with PNR data," as has been the case in South Africa.[21]

It is important to note that the information in a PNR can vary, but generally includes information such as a passenger's name, date of birth, address, passport information, telephone numbers, and information related to the means of purchase. Each PNR is different, depending on the information provided, what airline is collecting the data, and the security concerns of a given country. In 2003, the European Commission stated that there were "20–25 possible fields of PNR data, some of which include subsets of information, expanding the total to approximately 60 fields and sub-fields."[22] The data that is collected is dependent on a specific country's legislation, airline regulations, and whether or not 'optional' fields are included. As such, passenger data can include information from Other Service Related Information (OSI), Special Services Information (SSI), and Special Service Requests (SSR),[23] which can include a range of information including medical services, physical as well as medical conditions, religious beliefs, or other sensitive data.[24] Under these categories – SSI and SSR – additional information is entered, though it is not required to purchase the ticket. This information may also include seat assignment, meals, health and accessibility concerns, etc. and some fields may be shared with other carriers through an interoperability mechanism.[25] Once a PNR is created it has an audit trail, that is, a chronological succession of data recording each entry or change to the PNR, including information on location, time, and the user ID of employees, travel agents, and airline staff who edited or added to the PNR.[26]

The collection of PNR related information represents "one of the most detailed and personal data sources"[27] that can be used by states for the pre-emptive and predictive risk management of mobile populations. Interestingly, once PNR data is processed, a significant amount of additional information can be deduced from the fields. A PNR can effectively

> [s]how where you went, when, with whom, for how long, and at whose expense. Behind the closed doors of your hotel room, with a particular other person, they show whether you asked for one bed or two. Through departmental and project billing codes, business travel PNR's reveal confidential internal corporate and other organization structures and lines of authority and show which people were involved in work together, even if they travelled separately. Particularly in the aggregate, they reveal trade secrets, insider financial information, and information protected by attorney-client, journalistic, and other privileges.[28]

While the information that a PNR contains has been willingly provided by a passenger, the data that a PNR encompasses is inherently sensitive. PNRs are non-discriminatory; along with potentially making it easier to detect terrorists and criminals, it impacts all passengers regardless of age, nationality, or status. Thus, while PNR data is a valuable tool for national security, it also presents potential for misuse if not protected appropriately.

---

[15] Convention on Civil Aviation ("Chicago Convention"), Dec. 7 1944, 15U.N.T.S. 295. https://www.icao.int/publications/Documents/7300_orig.pdf.

[16] Chicago Convention, Chapter V, Article 29(f).

[17] Andrew Byrne, "Building the Transatlantic Area of Freedom, Security and Justice. The Case of the Passenger Name Record Agreements." *Istituto Affari Internazionali*, March 06, 2014, 1-18.

[18] Ibid., 4.

[19] Ibid., 5.

[20] Ibid.

[21] Ruwantissa Abeyratne. *Aviation Security Law*. Berlin: Springer Berlin, 2010. 125–6.

[22] European Commission, "Airline Passenger Data Transfers from the EU to the United States (Passenger Name Record) Frequently Asked Questions," European Commission: Press Releases, Memo/03/53, March 12, 2003, http://europa.eu/rapid/press-release_MEMO-03-53_en.htm.

[23] ICAO, *PNR Guidelines*.

[24] This information may be directly provided or deduced from the information provided.

[25] Colin J. Bennet, "What Happens when you Book an Airline Ticket? The Collection and Processing of Passenger Data Post-9/11," in Zureik and Salter, *Global Surveillance and Policing*, 2005: 113–38. cf. Zureik, Elia, and Mark B. Salter, eds. *Global Surveillance and Policing: Borders, Security, Identity*. Portland, OR: Willan Publishing, 2005.

[26] Ibid., 117.

[27] Paul De Hert and Rocco Bellanova, "Transatlantic Cooperation on Travelers" Data Processing: From Sorting Countries to Sorting Individuals (Washington DC: Migration Policy Institute, 2011), quoted in MatthiasLeese, "The New Profiling: Algorithms, Black Boxes, and the Failure of Anti-discriminatory Safeguards in the European Union." *Security Dialogue* 45, no. 5 (2014): 497.

[28] Hasbrouck, "What's in a Passenger Name Record?", np.

3. PNR overview in South Africa

The 2014 amendments to the South African Immigration Act 13 of 2002, Section 34(5) of the Immigration Regulations, require that every aircraft submit PNR information to the government electronically.[29] This applies to every person travelling to, from, and within South Africa. The PNR information required by South Africa includes:

> (a) the date of reservation; (b) the dates of intended travel; (c) the first name and surname; (d) other names on the passenger name record; (e) all forms of payment information; (f) the billing address; (g) the contact telephone numbers; (h) all travel itineraries for that specific passenger name record; (i) the frequent flyer information, limited to miles flown and addresses; (j) the travel agency; (k) the travel agent; (l) the split or divided passenger name record information; (m) the ticketing field information; (n) the ticket number; (o) the seat number; (p) the date of ticket issuance; (q) no show history; (r) the bag tag numbers; (s) the number of bags; (t) the record locator; (u) the weight of the bags; (v) the no show information; (w) the seat information; (x) whether the tickets are one-way tickets; (y) any information collected as contemplated in subregulation (2); (z) standby; and (aa) names of passengers who have been taken off the flight.[30]

According to the South African Revenue Service (SARS), only 10% of customs functions are performed at the port of entry in South Africa, whereas the majority of customs functions are performed pre- and post-border, outside of the physical territory of South Africa.[31] As such, the majority of the passenger sorting occurs through the use of PNR data which falls under this category of activities that are detached from the physical territory of the state; that is to say, the pre-examination of passengers through the use of PNR takes place before they reach South African territory. This data is sent to the APP system[32] whereby the collected data is checked against the Department of Home Affairs' (DHA) records and "the business rules in the system and returns a directive to the airline whether or not to board the passenger".[33]

The APP system cross checks passengers against Interpol lists and several lists provided by the South African DHA including; DHA Visa and Entry Stop (V-List), South African passports issued, lost and stolen South African passports, and South African visas issued, to detect the status of a traveller before boarding.[34] The DHA V-list is described as "a list that takes on a life and questionable legality of its own, courtesy of the Department" and consists of the names of individuals who are not welcome in the country.[35] What is most interesting is that "it appears that persons can be 'V-listed' at the request of foreign or international police agencies and it is not unknown for those bodies to err".[36] In the event that there is a positive match, the airline has an opportunity to consult the DHA operational center in South Africa to verify the inadmissibility of a passenger, and a government override could be performed.[37] An example of the potential of such a system can be seen in the fact that 623 travellers were denied boarding on flights to South Africa by various airlines between December 9, 2016 and January 14, 2017.[38]

South Africa's implementation of its own PNR regime for the purpose of pre-screening prior to immigration clearance has been praised by the ICAO, noting that South Africa has received a clean audit (related to Annex 9 of the Chicago Convention) and that the country has excelled in its adoption and implementation of PNR.[39] South Africa has met the international standards in terms of the transmission of this data, the elements that it collects, and in limiting administrative and operational burdens related to the system.[40] It is noteworthy that South Africa's implementation of PNR was not a replica of another country's PNR regime and involved the transmission of not only passenger record fields but also Advanced Passenger Information System (APIS) data. This is reflected in the 2014 amendments to the South Africa Immigration Act (2002) to enforce the mandatory transmission and use of Advanced Passenger Processing (APP), and the inclusion of PNR data shortly after.[41] As previously stated, South Africa is the first country on the African continent to implement a PNR system, and is one of only thirteen international states to link their API and PNR systems.[42] This action reflects the ambitious security practices the country has adopted and is an important move to enhance South Africa's border security. In fact, the ICAO has ranked South Africa as number one in terms of aviation security on the continent and number 33 globally.[43]

---

[29] *Government Gazette* 37679, Immigration Act, 2002. Immigration Regulations (2014 amendments)., Regulation Gazette 10199, 22 May 2014 [South Africa], No. R.413. http://www.gov.za/documents/immigration-act-regulations-immigration.

[30] Ibid., Section 34(2).

[31] Department of Home Affairs Summary of the Customs Value Chain and the Proposed Role for the BMA, Confidential, 23 Sept. 2016. https://pmg.org.za/files/161018OVERVIEW_OF_THE_SARS_CUSTOMS.docx.

[32] Which includes PNR data

[33] Department of Home Affairs, "Presentation To The Portfolio Committee On The Status Of Ports Of Entry And Asylum Seekers Management", PowerPoint presentation, [South Africa] May 22, 2012. https://pmg.org.za/files/docs/120522status.ppt.

[34] Ibid.

[35] Bregmans. "Visas and Entry into South Africa." May 09, 2014. https://www.bregmans.co.za/visas-and-entry-into-south-africa/.

[36] Ibid.

[37] Department of Home Affairs, "Presentation To The Portfolio Committee".

[38] Dorine Reinstein, "South Africa about to Become Family-Friendly Again. Or Is It?" September 28, 2018. https://www.travelweekly.com/Middle-East-Africa-Travel/Insights/South-Africa-about-to-become-family-friendly-again-Or-is-it.

[39] ICAO, "ICAO Regional Facilitation Seminar", February 2014. https://www.icao.int/ESAF/Documents/meetings/2014/FAL-FEB/SOUTH%20AFRICA-Annex%209-Facilitation%20and%20Implementation%20Status.pdf.

[40] Ibid.

[41] Immigration Act, 2002 (2014) cf. Immigration Regulations (2014).

[42] Inside MRO, "There Is Still Hope For African Aviation."

[43] Nolan, Candice. "SA Ranked Number One in Africa in Terms of Aviation Safety." *SABC News*. May 22, 2017. https://www.sabcnews.com/sabcnews/sa-ranked-number-one-in-africa-in-terms-of-aviation-safety/.

4. South African data protection: the POPI act

Following a global trend toward state adoption of privacy legislation, on the 19th of November 2013, South Africa implemented the Protection of Personal Information Act (POPI) No.4.[44] Prior to this date the country did not have clearly articulated privacy legislation[45]that could protect individuals from new technology that might impact how personal information is collected, stored, processed, and transferred.[46] The intention of the legislation is to protect personal information collected and processed by both the public and private sectors - including the government - and to develop the necessary institutional bodies to ensure compliance with the act. In effect, the POPI Act would help protect the basic privacy rights already guaranteed in the South African Constitution - "everyone has the right to privacy"[47] - in an era when technology is making it increasingly difficult to do so. The POPI Act provides a high level of protection to personal data as it is designed to: ensure that the responsible parties are using sufficient safeguards when processing personal data; regulate how personal information can be legally processed through the clear establishment of conditions which were inspired by international standards; provide individuals with clear rights and remedies to protect their personal data; and to establish clear standards of compliance for responsible parties.[48]

In December of 2016, an Information Regulator was appointed by the President of South Africa to enforce the POPI Act to ensure the right to privacy and the protection of personal data.[49] The Information Regulator is responsible for a range of activities related to the POPI Act including: educating responsible parties about the protection of private information, monitoring and enforcing full and proper adherence to the act, managing complaints regarding potential privacy violations, researching issues into codes of conduct, and facilitating cross border data sharing and cooperation when necessary. There are severe consequences in place to deter any public or private entity from failing to comply with the POPI Act. In the event that there is a failure to comply, the Information Regulator has authority under sections 107 and 109 to impose fines (up to R10 Million) and imprisonment (not exceeding 10 years) or a combination thereof to the guilty parties.[50] In principle, the Act should significantly influence how personal information is collected, stored, saved, used, and shared in the country; however, the full implications of the Act are not yet clear because while the act officially came into effect on July 1, 2020, full enforcement of the Act will not take place until July 2021.[51]

Under the POPI Act, there are eight conditions for the legal processing, storage, and transfer of personally identifiable information.[52] The first condition is accountability[53]; it is up to the responsible party to guarantee that all conditions of the Act are met to ensure the lawful processing of personal data. The second condition refers to data processing limitations; this condition attests to the need of each responsible party to lawfully process personal information in a manner that will not infringe on the privacy of the data subjects.[54] In addition, this condition requires that data is collected directly from the data subject and that the responsible party must ensure that the personal information is processed for the purpose collected, that its collection is not excessive, and that there is opportunity for consent, justification and objection.[55] The third condition relates to specificity of the data; personal data must be collected for a specific purpose which is explicitly defined, and the lawful party must ensure the data subject is aware of the data collection and purpose.[56] The fourth condition deals with further processing limitations by ensuring that the processing of data is compatible with the original purpose of data collection as outlined in condition three of the Act.[57] The fifth condition is related to information quality; it is the responsible party's obligation to ensure that appropriate measures are taken to guarantee that the personal data collected is reliable, complete, accurate, not misleading, and updated as necessary.[58] The sixth condition speaks to openness and transparency; the data subject ought to be notified when their personal data is being collected and the responsible party must retain documentation of its processing operations.[59] The seventh condition speaks to security safeguards that the responsible party must adopt in order to ensure the integrity and confidentiality of the collection of personal data.[60] The eighth, and final condition concerns data subject participation and states that data subjects have the right to access their own personal information.[61] These eight conditions as outlined in the Act are similar to the leading international standards, however, the South African POPI act provides increased, additional protection of 'special'(sensitive) personal information which includes information concerning children,[62] a person's religion/ philosophical beliefs, race, ethnic origin, political opinions, health, biometric data, sexual life, and criminal

[44] POPI Act.
[45] Cf. Limited data protections found in the Promotion of Access to Information Act (Act 2 of 2000), Electronic Communications and Transactions Act (Act 25 of 2005), and the National Credit Act (Act 32 of 2005).
[46] POPI Act.
[47] *Government Gazette* 17678, Section 14 of the Bill of Rights of the Constitution of the Republic of South African, 1996.
[48] POPI Act.
[49] POPI Act. Cf. "Members of Information Regulator Appointed." *The SA Government News Agency*. October 26, 2016. https://www.sanews.gov.za/south-africa/members-information-regulator-appointed.
[50] POPI Act, Chapter 11 (107-109).
[51] John Giles, "When is the POPIA deadline in South Africa?" *Michaelsons*, June 22, 2020. https://www.michalsons.com/blog/when-is-the-popia-deadline-in-south-africa/39672.
[52] POPI Act, Chapter 3.
[53] Ibid. Condition 1.
[54] Ibid., Condition 2.
[55] Ibid.
[56] Ibid., Condition.3.
[57] Ibid., Condition 4.
[58] Ibid., Condition 5.
[59] Ibid., Condition 6.
[60] Ibid., Condition 7.
[61] Ibid., Condition 8.
[62] Anneliese A Roos," Data Protection Law in South Africa". In: Makulilo A. (eds) *African Data Privacy Laws*. vol 33. Springer, (2016): 206.

behaviour.[63] However, there are substantial exclusions outlined in the POPI act which seem to suggest that while PNR data used for commercial purposes is protected, this protection does not extend to PNR data used for national security purposes.[64]

It should also be noted that the POPI Act was intended to align South African privacy laws with the leading international standards. The POPI Act was designed by the South African Law Reform Commission - an independent advisory statutory body - after careful examination of global privacy laws[65] and therefore closely reflects the privacy standards of the Organisation for Economic Cooperation and Development (OECD) and the European Union (EU) Directive.[66] While the POPI Act uses a slightly different vocabulary – 'personal information'[67] (personal data), 'responsible party'[68] (data controller), 'operator'[69](data processor), and 'conditions'[70] (principles) of lawful processing - there is no substantial evidence that these terms vary in meaning.

4.1. *The POPI act and South Africa's use of PNR*

PNR data is considered to be personal information in South Africa and should be protected under the POPI Act 4 of 2013 and the Act's regulatory framework that applies to the processing of personal information. Under the POPI Act, personal information is described as any information related to an identifiable living person, and includes: race; gender; sex; nationality; age; health; language; information related to medical, financial, or criminal history, and employment; and email addresses, physical address, telephone numbers, biometric information, etc.[71] The POPI Act, therefore, should apply to all aspects of PNR collection, storage, and use in South Africa according to Section 19 of the Act which guides the processing of Information. Further, Section 72 of the POPI Act guides the security and confidentiality of data with respect to its transfer outside of the country and should therefore apply directly to the country's PNR regime. However, there are exclusions outlined in the POPI Act which indicate that while the commercial use and processing of PNR data is protected, the Act does not apply to the processing of personal information used by public bodies for national security purposes "to the extent that adequate safeguards have been established in [other] legislation for the protection of such personal information."[72] Interestingly, neither the POPI Act nor the government has provided any clear indication as to what specific legislation can protect the privacy of PNR data when it is used for national security purposes.

Section 19 of the POPI Act responds to the processing of personal information and places the obligation for the security and confidentiality of data onto the party that has obtained the data and explains that they are responsible to take appropriate, reasonable, technical, and organizational measures to protect it.[73] Security of data includes protection from loss of data, damage to the data, unauthorized destruction or distribution of the data, and unlawful access to the data. As such, each entity that is responsible for the collection and storage of personal data must take measures to identify possible internal and external risks to the data, establish and maintain appropriate safeguards to protect the data from the identified risks, regularly confirm that the safeguards are effective, and ensure that they are updated to manage new risks.[74] Further, the responsible parties must accept information security practices and procedures that may apply. The POPI Act effectively ensures that South African institutions have harmonized procedures for collecting and processing personal information and it holds these entities accountable for the proper protection of data. However, there is no clause that speaks specifically to PNR data or that ensures its protection under these standards.

As noted, Section 72 of the POPI Act addresses the transfer of data outside the country.[75] Personal information may not be transferred to a third party located outside of South African borders unless: the third-party recipient is subject to laws which provide sufficient protection of the data; the law has provisions which are similar to South Africa's law related to the transfer of personal information outside of state borders; the subject consents to the transfer; the transfer of the data is deemed necessary; and/or the transfer is of benefit to the subject.[76] Exceptions to this section include third parties who are subject to law binding corporate rules, or binding agreements which have adequate levels of protection. While these areas of the POPI Act appear to be adequate at first glance, the Act is particularly elusive as it relates to transferring data to a third party located outside of South African borders other than that the third-party recipient must be subject to laws which provide sufficient protection of the data. Under the POPI Act, the organization that intends to transfer data outside of South Africa is obligated to adhere to specific security requirements to ensure that shared data is protected from unauthorized use and that the level of security is adequate to both the nature and sensitivity of the data in hand. However, the POPI Act does not provide clear information related to which countries have adequate levels of protection or how these countries can be identified; in the case of PNR, this suggests that the data can be transferred wherever South Africa wants to send it, especially considering that most countries have, or are implementing data laws similar to, or more advanced than South Africa.[77]

[63] POPI Act. Chapter 3, Condition 8, Part B.
[64] POPI Act Chapter 3, Condition 2. Cf. Section 6(1)(c) and Section 37(1-2).
[65] Michelle De Bruyn, "The Protection Of Personal Information (POPI) Act - Impact On South Africa." *The International Business & Economics Research Journal* (Online) 13, no. 6 (May 11, 2014). 1316.
[66] Ibid.
[67] POPI Act, Chapter 1.
[68] Ibid.
[69] Ibid.
[70] Ibid., Chapter 3.
[71] Ibid., Chapter 1.
[72] POPI Act, Chapter 2, Section 6.
[73] POPI Act, cf. Chapter 3, Chapter 9.
[74] Ibid., Chapter 3, Condition 7 (19).
[75] Ibid., Chapter 9 (72).
[76] Ibid.
[77] The increase in global adoption of privacy laws is closely related to Article 25 of the European Union's 1995 Data Protection Directive which prevents EU member states from transferring personal data to countries that do not have adequate level of data protection.

While the POPI Act appears to provide substantial data protection, there are currently no laws that explicitly restrict or limit the international transfer of personal information, including PNR data, outside of South Africa.[78]

The POPI Act does not necessarily provide any protection to PNR data used by the state for security purposes. This is because the POPI Act has substantial exceptions including the fact that the Act may not apply when personal information is used for national security or for policing.[79] The POPI Act permits non-compliance if the action is "in the interests of national security".[80] The exception for national security then is incredibly broad and includes activities related to the identification or financing of terrorist related activities, and for the defence of public security.[81] Further, the POPI Act exempts those acting for or on behalf of a public body in the prevention and detention of unlawful activities, investigation of offences, and prosecution of offences.[82] Therefore, it is not clear to what extent PNR data used by the South African state is protected by the POPI Act given that PNR is used for legitimate national security purposes, and that there are no other laws which specifically cover PNR data protection. In lieu of the government providing a clear purpose for its use of PNR and to provide public information on how the data is protected, it can be presumed that all PNR data collected and stored by airlines for commercial purposes will be protected by the POPI act, but this does not necessarily extend to the same PNR data used by the state for security purposes. It is therefore very possible that the use of PNR data by the state for national security purposes falls outside the protection of the POPI Act, and that the data has no significant legal protection domestically or when transferred to a third country.

Although the POPI Act should apply directly to PNR data, specific laws related to PNR data protection are imperative because the use of PNRs for security purposes effectively represents an intersection of security and rights. The lack of provisions and safeguards for personal information has an impact on the fundamental rights of individuals, particularly because commercial airlines and travel agents use third-party Global Distribution Systems to collect personal data that will be used for two different purposes; business purposes for commercial airlines and security purposes for the state.[83] Under these circumstances, it is crucial that "if the right to privacy of individuals is to be protected, then we cannot anymore only think of the responsibility of the state."[84] The concern about the lack of laws that specifically address PNR data is important because there are a number of public and private actors involved in the collection, storage, and use of PNRs in South Africa, and there is uncertainty about the extension of the "fundamental rights obligations to the private sector and the exact scope and contour of their duties."[85] The impact of these interactions result in the fundamental rights of individuals no longer needing protection only from the state, but also from private corporations.[86] However, and somewhat ironically, the POPI act clearly applies to private corporations but may exempt the state from having equal responsibility.

In short, the POPI Act is a legal mechanism that has the potential to bring the protection of personal data in South Africa in line with international standards, but there remains an evident "lack of enforcement mechanisms at present to give effect to such transnational, universal obligations."[87] Notwithstanding the honourable intentions of the POPI Act, the fact remains that in some cases there is a need for more exclusive legislation related to the protection of the PNR data of both citizens and non-citizens, beyond the protection that may or may not be available in the POPI Act.

5. Other South African data protection laws: customs and immigration regulations

Given the ambiguous status of the POPI Act's applicability to the protection of PNR data and the South African government's failure to provide clear public information regarding the protection of personal data, it is important to briefly consider protection of personal data that may come from other legislation in the country. However, it is important to note that the ICAO provides guidelines as to how states that use PNRs can help guarantee the protection of personal information. This includes, but is not limited to, the notion that there should be limited access to, and limited retention of, PNR data.[88] Currently, South Africa does not explicitly provide this information. Rather, PNR data may be permanently stored in South Africa, and done so without publicly available information on who has access to the data, how this data is protected, or under what circumstances it may be transferred.

Once again, the status of PNR data protection remains somewhat cryptic and the 'fine print' is difficult to interpret. The POPI Act effectively states that protections granted under the Act do not apply to personal information used for national security purposes in the case that the data is protected by another relevant piece of legislation.[89] For example, such a piece of legislation could include the Customs and Excise Act. When speaking directly about PNR data protection, a representative of the South African Customs department stated that "the collection and handling of passenger information is for customs purposes and is protected under Section 4 of the Customs and Excise Act meaning that passenger data cannot be disclosed or discussed with any third party."[90] However, Section 4 of the

[78] Theo Ling, ed., "Global Privacy Handbook: Global Privacy and Information Management Handbook 2018". (Chicago, IL: Baker McKenzie, 2018), 633.
[79] Right2Know(R2K), "POPI Guide – Protect Your Private Info." Right2Know Campaign, https://www.r2k.org.za/popi-guide/.
[80] Specifically, the POPI Act Chapter 3, condition 4(3) and Condition 6(1)(a)-(e) states that the POPI Act does not apply when the activities are a matter of national security.
[81] POPI Act Chapter 2, Exclusions 6(1)(a)-(e)
[82] Ibid.
[83] David Cole, Federico Fabbrini, and Stephen J. Schulhofer, *Surveillance, Privacy, and Trans-Atlantic Relations*, Hart Studies in Security and Justice, vol. 1 (Oxford, UK: Hart Publishing, 2017).
[84] Ibid.,114.
[85] Cole et al., *Surveillance*, 116.
[86] Ibid.
[87] Ibid., 135.
[88] ICAO, *PNR Guidelines*.
[89] POPI Act, Chapter 2 and Chapter 10.
[90] Email message to the author, January 9, 2018.

Customs and Excise Act (1964) provides virtually no protection to PNR data that is used for security purposes.

Although the original Customs and Excise Act has been updated several times, it is still not easy to understand if and how it provides protection to personal information.[91] The applicable clause in the legislation states only that: "No officer shall, except for the purposes of this Act or when required to do so as a witness in a court of law, disclose any information relating to any person, firm or business acquired in the performance of his duties."[92] If this is the case, and PNR data used by the state is protected by the Customs and Excise Act, not the POPI Act as indicated by South African Customs, it becomes incredibly problematic because Section 4 infers a restriction on the disclosure of data but does not limit the state's use of PNR data for mass surveillance or data mining. In short, the Act provides little to no protection for a state's use or misuse of PNR data, nor does it protect the personal information of individuals in any capacity as it relates to state use of the data, and therefore should not validate a justified exemption from the protection of the POPI Act.[93] It is impossible to ignore the lack of publicly available information regarding South African use of PNR and the ambiguous status of PNR protection in the country. Simply, if PNR data falls outside of the POPI Act because of its use for national security, there is virtually no significant protection provided to this data under the Customs and Excise Act.[94]

There is a small amount of protection afforded to PNR data as outlined in the 2014 Amendments to the South African Immigration Act 13 (2002). Immigration Regulations Section 34(8) explicitly identify safeguards and protection measures for PNR data in that the Director-General will employ appropriate security measures that ensure the integrity of personal data, including confidentiality of the data and protection against unlawful access. This section of the act also safeguards data against disclosure, unless required by law. Finally, the Immigration Regulations suggest that the Director-General is responsible for the security of personal information and for turning to relevant law enforcement agencies if personal data has been accessed or acquired by unauthorized persons. However, specific definitions are not provided in the Act and the result is that the limits of the protection of personal data remain vague. There is a failure to provide specific limitations on the access and internal sharing of the data, as well as a failure to provide definitions, and thus it is not clear what is meant by statements such as "unauthorized," "relevant law enforcement," and so on.

6. South Africa's PNR regime – in line with international standards?

South Africa's POPI Act draws attention to the responsibility of both public and private actors in the protection of an individual's personal data. The Act is important in a globalized world wherein an individual's data is being collected, processed, and shared among a myriad of networks, servers, and algorithms of multiple governmental and private actors.[95] Although South Africa's POPI Act is considered to be of a high standard in terms of privacy protection,[96] and South Africa is "regarded as a country in which regulation and enforcement are moderately applied",[97] there is not enough evidence to suggest that the POPI Act provides an adequate level of data protection to the state's use of PNR data.

In this section, South Africa's PNR regime will be analyzed with specific attention paid to the European Union (EU) standards[98] for PNR and privacy protection. Whereas there is minimal public information on the South African PNR regime in terms of its official use and data protection, the EU is recognized for its high level of data protection[99] and there are considerable public documents related to its PNR use. This includes the EU Directive,[100] the United States (US) –EU Agreement on Passenger Name Records,[101] and the decision on the EU-Canada Passenger Name Record Agreement.[102] These documents provide clear and public insight into PNR data use and transfer with respect to the right to privacy of the data subjects

[91] SARS. "Questions & Answers - New Customs Legislation." SARS Online. [South Africa] November 29, 2018. https://www.sars.gov.za/ClientSegments/Customs-Excise/AboutCustoms/Pages/Q-and-A-for-the-new-Customs-Legislation.aspx.

[92] Customs and Excise Chapter Act 2 (4)(3)

[93] The POPI act states that the laws do not apply when the personal information is being used for security purposes, but only if the data is protected by another law. The 'New Customs Act' does not protect PNR data from privacy abuse.

[94] Ultimately, the 1964 Customs and Excise Act has "not kept pace with the changing pace of customs work or …. The rapid growth in the use of information technology and the exchange of electronic data" (SARS, New Customs Legislation. np,). In 2003, SARS began to re-write and modernize the Act to clarify its legislative framework. Although the updated Acts (now the Customs Control Act, the Customs Duty Act, and the Customs and Excise Amendment Act) were published in 2014, they have not yet come into force and no date has been established. cf. SARS. "New Customs Legislation Update" *SARS Online*. [South Africa]. March 12, 2020. https://www.sars.gov.za/ClientSegments/Customs-Excise/AboutCustoms/Pages/New-Customs-Legislation-update.aspx.

[95] Cole et al., *Surveillance*.

[96] Roos, *Data Protection Law in South Africa*, 206.

[97] DLA Piper, 2018 cited by Da Veiga, A., Vorster, R., Li, F., Clarke, N. and Furnell, S.M. (2019), "Comparing the protection and use of online personal information in South Africa and the United Kingdom in line with data protection requirements", *Information and Computer Security*, Vol. 28 No. 3, 400.

[98] Noting that the EU has not yet recognized South Africa as having adequate data protection laws.

[99] Privacy Europe. (n.d.). "European Privacy Framework". Retrieved from https://www.privacy-europe.com/european-privacy-framework.html.

[100] "Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime," *Official Journal* L 119, 4.5.2016, 132–149.

[101] European Data Protection Supervisor. Opinion of the European Data Protection Supervisor on the proposal for a council decision on the conclusion of the agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security; *Official Journal* C 35, 9.2.2012,16–22.

[102] Opinion 1/15. Draft agreement between Canada and the European Union — Transfer of Passenger Name Record data from the European Union to Canada. *Official Journal*. C2017, 592.

being protected.[103] In order to make a meaningful evaluation, the South African PNR regime will be compared to the EU standards in terms of the scope and use of PNR data, data security, oversight, transparency, access, retention, domestic sharing, and international sharing.[104]

6.1. *Use of PNR data*

The EU severely restricts the global transfer of PNR data to a case-by-case basis; the transfer must not exceed what is necessary for the purpose of the transfer and the third country cannot reduce the degree of protection provided by EU law.[105] According to the EU, PNR data should only be used to prevent, detect, investigate, and prosecute terrorism or other serious crimes.[106] There is an explicit expectation that states will clearly indicate the intended use of PNR data which should be limited to the proactive and repressive efforts related to terrorism, security threats, and serious crime, but may also include investigation of more general crimes.[107]

Without a clear statement indicating how and why PNRs are used for national security purposes in South Africa, it may only be assumed that PNR use represents the state's "desire to prevent terrorism".[108] While PNR is widely used in Europe and North America to improve border security and to prevent terrorist activity,[109] unlike these regions, South Africa has no known significant threat to national security, especially terrorist threats.[110] There is currently no information clearly indicating which bodies in South Africa might have access to PNR data for any purpose let alone to prevent, detect, investigate, and prosecute terrorism and serious crimes. This is problematic insofar as South Africa has not clearly revealed the purpose for its PNR data use - even in the Immigration Regulations (2014), Section 34.5 - nor is there disclosure in terms of access or aims of use of the data as indicated under Section 13 of the POPI Act.

Rather than aligning itself more closely with international standards on PNR and data protection, South Africa has not yet provided a public explanation for the use of PNR. In fact, the only public account of the country's intentions with respect to its PNR use is found in the South African Revenue Service (SARS) five year strategic plan for 2016/17 to 2020/21 which focuses specifically on how South Africa intends to respond to international developments and how it will participate in the global system of governance. The document states that SARS is "working towards the implementation of various instruments of the World Customs Organization (WCO)"[111] including the Punta Cana Resolution.[112] The Punta Cana Resolution speaks directly to the role that customs officials play in international security and specifically, "the critical space they occupy at the border in the prevention of future terrorist attacks."[113] The SARS strategic plan specifically quotes the 2015 WCO Punta Cana Resolution;

> [The] Resolution calls on Governments and their Customs administrations to use the full range of detection and investigative techniques at their disposal, including risk profiling, Advance Passenger Information (API) and Passenger Name Records (PNR) analysis, intelligence sharing, controlled deliveries, forensic techniques, detector dogs and non-intrusive equipment, and upgrading them to high standards.[114]

Ultimately, this does not clearly indicate the use and purpose of their PNR regime, nor does it indicate how or if the data is being used to help prevent, detect, investigate, and prosecute terrorism and serious transnational crimes.[115] Currently, South Africa's PNR could be used for an extremely broad range of purposes and activities unbeknownst to the public.

Of further concern is that while the EU PNR requirements are explicit in that PNR data should not be used for purposes other than for terrorism or serious crime, there is evidence that South Africa uses it for migration control as a means to apply a 'first safe country' concept, without a formal legal basis to do so, to asylum seekers not arriving from bordering countries:

> [I]t appears that the safe third country and country of first asylum concepts hidden in the newly introduced advance passenger processing act as automatic bars for asylum applicants who do not enter South Africa directly from the country of origin. This effectively limits access to asylum in South Africa to applicants from neighbouring countries.[116]

What is of interest in suggesting that PNR data may be used to prevent legitimate asylum claims is the reality that the country's 1998 Refugees Act does not incorporate the terms

[103] The EU court ruled that the EU-Canada PNR Sharing breached European law in the Court of Justice of the European Union Opinion 1/15 as being incompatible with right to privacy (Article 7), right to data protection (Article 8), and principle of proportionality (52) of the Charter of Fundamental Rights of the European Union.

[104] European Data Protection Supervisor (EDS) highlighted these categories in reference to transatlantic data sharing agreements. Cf. Olga Mironenko Enerstvedt, "Russian PNR System: Data Protection Issues and Global Prospects," *Computer Law & Security Review*: The International Journal of Technology Law and Practice 30, no. 1 (2014).

[105] Cf. Directive (EU) 2016/681, Article 11 - Article 13.

[106] Cf. Directive (EU) and US-EU Agreement on PNR, Article 4, Article 18.

[107] Ibid.

[108] Hammarberg, *Protecting the Right to Privacy*, 2.

[109] Leese, Matthias, "The New Profiling", 494–511.

[110] Duncan, Jane. *Stopping the Spies: Constructing and Resisting the Surveillance State in South Africa* Baltimore, Maryland: Project Muse, 2018,12.

[111] SARS, *Strategic Plan 2016/17 - 2020/21*, prepared by the South African Revenue Service (South Africa), 21. https://www.sars.gov.za/AllDocs/SARSEntDoclib/Ent/SARS-Strat-18%20-%20Strategic%20Plan%202016%202017%20to%202020%202021%20-%205%20September%202016.pdf.

[112] In the aftermath of the A321 crash of a Russian plane over Egypt, and the consequential ruling as a terrorist attack, in 2015 the WCO issued a resolution titled the Punta Cana resolution (UNSCR 1540). The resolution speaks directly to improving customs and enhancing border security capabilities.

[113] SARS *Strategic Plan 2016/17 - 2020/21*. 24.

[114] Ibid., 24.

[115] Cf. US-EU Article 4.

[116] María-Teresa, Gil-Bazo. "Responses to Secondary Movements of Refugees: A Comparative Preliminary Study of State Practice in South Africa, Spain, and the USA," (Discussion paper prepared for UNCHR Expert Meeting on International Cooperation to Share Burdens and Responsibilities, Amman, Jorden, 27-28 June 2011), 6.

'safe third country' or 'country of first asylum'.[117] As such, PNR data can allow pre-emptive rejection of asylum applications which could not be done on South African territory due to the lack of a legal basis. PNR is a means for the government of South Africa to implement and apply the 'first safe country', 'safe third country', and 'country of first asylum' rules. Specifically, the DHA has publicly stated that pre-screening will not take place when South Africa is the first safe country when entering from the countries of origin (this limits asylum seekers to countries South Africa shares a border with).[118] Simply stated, there is evidence that PNR data is being used by the government to manage the secondary movement of refugees, prevent their arrival in South Africa to claim asylum, and in doing so, risks violating the international non-refoulement principle.[119]

It is important to note that the US-EU PNR Agreement states that PNR data may be used on "on a case-by-case basis where necessary in view of a serious threat and for the protection of vital interests of any individual or if ordered by a court" to identify persons of interest for closer examination, and thus implying the use of PNR could include a large number of minor crimes that are not directly related to terrorism.[120] However, South Africa's potential use of PNR to enforce a safe third country rule, where there is no legal foundation to do so, would certainly be deemed excessive and inappropriate when compared to international standards.

6.2. *Data security*

The ICAO[121] and the EU[122] both identify the need for the use of PNR data to be protected from misuse and unlawful access. To ensure the protection of personal data, the EU strategy requires that the appropriate technical and security measures be implemented in order to mitigate risks to the security, confidentially, or integrity of the data. South Africa's POPI Act provides security safeguards to ensure the confidentiality and integrity of personal information and to protect the data from unlawful access and processing.[123] However, unlike the EU, there are no clear decisions or directives that speak directly to the security of PNR data in South African law.

As mentioned previously, Section 34(8) of the South African Immigration Regulations, 2014 provides some information on the protection of PNR data. It is clearly stated that PNR data is to be transmitted to the "Director-General through the communication channel provided by the Director-General"[124] and the Director General is to apply the necessary security measures to maintain the confidentiality of data and to protect it against unlawful access.[125] The Regulations also state that PNR data will remain confidential unless otherwise required by law, and that the relevant authority will ensure that the individual who processes the information does so in accordance with security measures.[126] Finally, it is noted that relevant law enforcement agencies will deal with breaches of the above safeguards.[127] However, what exactly constitutes a breach of security or which law enforcement agencies are to deal with these types of incidents also remains elusive.[128] This is particularly important in the case of South Africa because while the POPI Act brings the privacy of South African personal information in line with international law, the country is noted to be ranked third in the world in terms of being victim to cybercrime.[129] Given the high number of cybercrimes in the country, it would be expected that the government not only have clear and enforceable data protection laws, but also clearer information regarding the security measures being taken to protect personal data in the country.[130]

Although the efforts to ensure PNR data security in South Africa remain vague, they seem to be largely aligned with international standards. However, given that the entire PNR regime operates in the absence of public information about if and how PNR data that is used by the state for security purposes is protected, it is difficult to know if this is true in practice.

6.3. *Oversight and accountability*

Oversight and accountability have been strongly incorporated into the EU's PNR regime since its initial implementation. For example, each EU member state has to implement an independent data protection advisory authority that supervises the data processing of personal information to ensure the fundamental rights and freedoms of individuals are protected.[131]

---

117 Ibid., 4-8.
118 Ibid.
119 Ibid.,8.
120 US-EU Article 4(2).
121 ICAO, *PNR Guidelines*, 2.14 (4).
122 US-EU Article 5(4), Cf. Directive (EU) Article 5 and Article 6.
123 POPI Act, Chapter 3, Condition 7.
124 Immigration Regulations (2014), Section 34(3).
125 Ibid., Section 34(8).
126 Ibid.
127 Ibid.
128 See in comparison the EU standard: US-EU Agreement Article 5: and, European Data Protection Supervisor (2011) https://edps.europa.eu/sites/edp/files/publication/11-01-14_personal_data_protection_en.pdf.
129 Johnny Botha, M.M. Grobler, Jade Hahn, and Mariki Eloff. "A High-Level Comparison Between the South African Protection of Personal Information Act and International Data Protection Laws". 12th International Conference on Cyber Warfare and Security, Dayton, Ohio, March 3, 2017.58.
130 There has been research into the safety of PNRs found on CRS/GDS databases and these systems have been criticized for their outdated security measures, which make PNR data vulnerable. Research claims that GDS systems do not use two-factor authentication, but rather simply use a booking code to access PNRs. This puts the PNR information at significant risk of hacking, because a booking code is considered "weaker than a 5-digit password (<28.5 bits), which would be considered insecure for most applications". Karsten Nohl and Nemanja Nikodijevic, "Legacy Booking Systems Disclose Travelers' Private Information." *Security Research Lab*, December 27, 2016, https://srlabs.de/bites/travel-hacking/.
131 Directive (EU) Article 13 –15. Cf. Report From The Commission To The European Parliament And The Council On the review of Directive 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.COM/2020/305 final. https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20200724_swd-2020-128_en.pdf.

Under the directive, each member state also had to implement a Passenger Information Unit that is responsible for reporting any breaches in personal data.[132] This emphasis on oversight and accountability is further embedded in the General Data Protection Regulation of 2018 (GDPR) which states that each EU member state will establish at least one public authority responsible for ensuring that the rights and freedoms of the data subjects are not infringed upon. This emphasis is also reflected in Article 14 of the 2015 US-EU PNR Agreement which draws attention to the need for independent review and oversight of the agencies that use PNR data.[133] In short, EU law overlaps in a way that guarantees the protection of EU citizens, even when the processing occurs outside of the EU.[134]

South Africa, however, has no clear oversight of its PNR data beyond what may be provided by the POPI Act. This is rather limited compared to the EU standards because, as noted, protection of personal data under the POPI Act does not apply when authorities are dealing with matters of national security. Currently, the only indication of oversight in the Act is that the SARS Director-General is responsible for the security of PNR personal information,[135] however, there has yet to be a demonstration or proven record of autonomy or indication of powers of oversight, investigation, intervention, or review.[136] While the Director-General acts on behalf of the South African Government, a number of SARS staff members have been accused of serious corruption, bribery, mismanagement, and breaches of contract.[137] As such, the office of the Director-General cannot yet be considered an independent or trusted body.

Thus far South Africa has not explained or guaranteed the oversight of PNR data protection in any substantial or meaningful way. Internationally, oversight mechanisms are of significant importance in ensuring that the relevant authorities (currently unspecified in South Africa) with access to PNR data operate within the law, and that personal data is properly used and protected. Given the country's questionable surveillance history[138] and that inefficient oversight with respect to its intelligence services[139] and police services[140] has been a reiterating theme, it would not be surprising if there were weak oversight in relation to surveillance and PNR use. In which case, there could be implications involving unlawful activity related to the use of PNR data in mass surveillance.

In summary, South Africa fails to meet international standards in terms of oversight and accountability with respect to PNR data protection. Simply, South Africa has not established a specific body to provide oversight of PNR use in the country. Further, while the POPI Act established the Information Regulator as an independent body to monitor and enforce data protection similar to the Data Protection Authority in the EU, once again, South Africa has not provided clarity about PNR data use or whether or not the POPI Act can effectively monitor PNR data use in the country when its use falls under the umbrella of national security.

6.4. *Transparency and notice*

Both the ICAO[141] and EU[142] state that there ought to be transparency and a form of notification regarding the collection and use of PNR data. This requires that passengers are made aware that their personal data is being collected and used for security purposes, not only for commercial transportation purposes by the airlines.[143] This would generally occur at the time of purchase, and typically, the purchase of an airline ticket cannot be completed without submitting and agreeing to the collection of PNR data for security purposes.[144] Both the South African and EU[145] privacy law standards use an 'opt-in' consent and the collection of PNR data occurs at the time of ticket purchase. To purchase the ticket a person must indicate consent (typically by ticking a box before finalizing the purchase) and without which cannot continue with the transaction. As such, the transparency provision is fulfilled by all South African airlines in the collection and storage of PNR data in the airline operator's automated reservation system,[146] but currently the notice on the ticket is 'buried' within the contract that must be accepted by the passenger before purchasing the ticket. As such, South Africa is 'transparent' in the collection of PNR data, and this is reflective of the requirements for openness in the POPI Act[147]; however, most passengers are likely unaware that they have agreed to the collection and use of their personal data.

The prevailing concern with the South African PNR system, is the national security clause and lack of information regarding the use of PNR data for security purposes.[148] In

[132] Directive (EU) Article 4-5, cf. Article 13 –15.
[133] US-EU Article 14.
[134] Cedric Ryngaert and Mistale Taylor. "The GDPR as Global Data Protection Regulation?" *AJIL Unbound* 114 (2020): 5-9. Cf. GDPR 3(1) and 3(2).
[135] Immigration Regulations (2014), Section 34 (8).
[136] US-EU Article14 and the EU directive Article 15.
[137] Joe McGluwa, "Department of Home Affairs Riddled by Mismanagement Has Spent Millions in Legal Fees." Parliamentary Monitoring Group, July 18, 2019. http://pmg-assets.s3website-eu-west-1.amazonaws.com/Joe_McGluwa_BVS_Home_Affairs.pdf.
[138] Right2Know, *The Surveillance State: Communications Surveillance and Privacy in South Africa* (Cape Town, South Africa: The Media Policy and Democracy Project, March 2016), http://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/sa_surveillancestate-web.pdf.
[139] Brian Fikani Dube, "Accountability and Oversight of Intelligence Services in South Africa Post 1994" (MMPP thesis, University of Witwatersrand, 2013).
[140] Johan Burger, "After 20 Years of Democracy, South Africa's Police are Still Precariously Set Between the Risk of Complete Failure and the Challenges of Professionalism," *Institute for Security Studies: ISS Today*, June 27, 2014, https://issafrica.org/iss-today/policing-in-south-africa-it-doesnt-have-to-be-the-low-road.
[141] ICAO, *PNR Guidelines*, 2.14.
[142] US-EU Agreement, Article 10.
[143] Enerstvedt, "Russian PNR System", 36.
[144] Cf. Edward Hasbrouck, "What's in a Passenger Name Record?"
[145] EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.
[146] Abeyratne, *Aviation Security Law*, 122–51.
[147] Chapter 3, Condition 6 (17-19).
[148] POPI Act, Chapter 2, 6 (C).

fact, the POPI Act states that there are cases, generally associated to national security, whereby information can be used without proper permission.[149] For this reason, South Africa's surveillance system is generally considered to not respect the standards in place in North America and Europe[150] as it relates to personal privacy and data protection.[151] While there has yet to be significant discussion about the country's use of PNR (perhaps related to the failure to make that use publicly known), there has been some minor controversy linked to other surveillance mechanisms where there has been a noted lack of transparency. For example, despite the country's pledge to reform surveillance practices, it is well known that the South African government does not need to inform individuals if their communications are being intercepted or if their devices are being tracked, even without judicial authorization, so as to not jeopardize ongoing investigations.[152] Interestingly, "the data fields in PNRs with mobile phone information and credit card information obviously allow for easy linking of the PNR data to the other massive 'bulk' data collections held by the intelligence agencies, on global e-communications and financial transactions."[153]

In South Africa, the trend in surveillance appears to be that the government does not provide the public with any information on the subject and there is no expectation for transparency when activities are considered to be for security purposes. There is not enough information to confidently say that South Africa's use of PNR meets international standards in terms of transparency. On paper, South Africa seems to follow similar standards in terms of the commercial collection of PNR data, but the transparency regarding its use in terms of security remains ambiguous.

6.5. *Access*

Both the ICAO and EU state that an individual should be able to access their own PNR data. This is also recognized in the POPI Act under condition 8 (23) whereby data subjects, regardless of nationality or country of origin, have the right to access their personal data if it is appropriate to do so. However, where the EU has clear statements regarding an individual's access to their PNR data regardless of their nationality or country of origin, South Africa has no such public statement about how and where to access PNR data other than to say that a subject may request it.

The uncertainty over who has access to South Africa's PNR data is reflective of overall institutional trends in the country, thus making it incredibly difficult for individuals to request access to this information. It is simply impossible to know where to make the request. Further, there have been clear inclinations toward actors and institutions "becoming increasingly secretive, powerful and involved in political affairs" in the security cluster in the country.[154] As a result of the increase in security and the lack of clarity in this area, there has been a growth in access to information requests regarding South African intelligence under the country's Promotion of

Access to Information Act 2 of 2000.[155] These requests have sought for the government to publicly share "agreements, memoranda of understanding and/or other arrangements with foreign countries concerning the sharing between South Africa and/or its agencies and any other country and/or its agencies of information and intelligence" and to outline under which circumstances intelligence can be shared; the limitations of sharing intelligence; and the retention and use of information, among other related demands which could all include PNR data.[156] However, the State Security Agency (SSA) has not responded to many requests, notwithstanding that "inaction is deemed a refusal of the request under South African law," even after internal appeals.[157] While this is of concern, it may demonstrate the character of the government as it relates to respect and transparency of the law. Nearly half of all requests made under the access to information law in South Africa are refused or simply ignored.[158] This represents failure at the public and private levels in relation to constitutional access to information. Furthermore,

> The most common ground for refusal was that the records do not exist or cannot be found (Section 23 [of the Promotion of Access to Information Act 2 of 2000]). This is concerning because it speaks either to poor record keeping, and/or to the failure by public bodies to carry out duties which these bodies are required to undertake (since had these duties been carried out, records thereof would be available).[159]

These facts reflect poorly on the operation and organization of the South African government in this area. The uncer-

[149] Right2Know. "POPI Guide – Protect Your Private Info". Cape Town, South Africa: The Media Policy and Democracy Project, January 2019. https://www.r2k.org.za/popi-guide/.

[150] Simply, unlike the EU, Canada, or US, South Africa's security practices increasingly lean towards securitisation under conditions which provide few restrictions that would prevent abuse from state institutions. Cf. "State of Privacy South Africa." Privacy International. January 26, 2019. https://privacyinternational.org/state-privacy/1010/state-privacy-south-africa.

[151] John Giles, "UN Concerned about Privacy and Interception in South Africa." Michalsons, 18 Feb. 2019, www.michalsons.com/blog/un-human-rights-committee-concerned-about-privacy-and-interception-in-southafrica/19226.

[152] Right2Know, *The Surveillance State*.

[153] Douwe Korff and Marie Georges. "Passenger Name Records, Data Mining & Data Protection: The Need for Strong Safeguards." Strasbourg, France: Council of Europe, Directorate General of Human Rights and Rule of Law, June 15, 2015, 8.

[154] International Network of Civil Liberties Organizations (INCLO), *Surveillance and Democracy: Chilling Tales from Around the World*, (Geneva, Switzerland: INCLO, 2016) 105. http://www.inclo.net/pdf/surveillance-and-democracy.pdf.

[155] Avani Singh, "Access to Information Request in Terms of the Promotion of Access to Information Act 2 of 2000" Legal Resources Centre, (Johannesburg, South Africa: LRC Constitutional Litigation Unit, June 13, 2017), http://inclo.net/pdf/iisp/INCLO-LRC_request.pdf.

[156] Ibid.

[157] INCLO, *Surveillance and Democracy,* 101.

[158] Freedominfo.org, "South African Coalition Finds Weak Compliance With Law," Freedominfo.org: The Global Network of Freedom of Information Advocates, March 2, 2017, http://www.freedominfo.org/2017/03/south-african-coalition-finds-weak-compliance-law/.

[159] Access to Information (ATI) Network, *ATI Shadow Report,* 2016, 3. http://www.r2k.org.za/wp-content/uploads/CER-Shadow-Report-2016-Final.pdf.

tainty around whether or not they are willing to provide such information results in much ambiguity around the entire PNR regime and the integrated nature of government departments. As such, there is a lack of clarity about data protection as well as individual access to their data in this context.

If the POPI Act is applicable to PNR data, there are similar guidelines as the EU in terms of access to that data. However, South Africa has thus far not provided public details on their PNR regime in this regard and the country has consistently failed to respond to requests for personal access to PNR data.[160] Even if access to PNR data in South Africa were completed to EU standards insofar as "any individual, regardless of nationality, country of origin, or place of residence is entitled to request his or her PNR" data, this would generally be a weak provision.[161] It can be presumed that if this provision were applied to only the PNR fields, that most individuals would get access only to the information that they provided and are already aware of (name, data of birth, address, means of payment, seat number, etc.).[162] Rather, it would be more valuable if the individual had access to all personal data and related information, not simply the PNR data associated with any security investigation.

6.7. *Retention*

International standards of the retention of PNR data outlined both by the ICAO and the EU state that the retention of PNR data must not exceed what is necessary for the purpose of the collection of the data.[163] The EU directive 2016/681 states that all EU states are required to collect PNR data but this data is depersonalized after six months and deleted after five years, although it is vague in terms of stating what is classified as depersonalization, and in practice likely only acts as a limited protection. The US-EU PNR Agreement on the transfer of PNR data notes that the PNR data should be deleted after 5 years.[164] The US-EU agreement does have weaknesses, notably that data collected under Articles 4 (terrorism and transnational crimes) can be retained for periods that exceed 5 years[165] and that data "that are related to a specific case or investigation may be retained in an active PNR database until the case or investigation is archived".[166]

South Africa fails to provide any clear limitation on the retention of PNR data, even under the POPI Act. API however, falls under the Revenue Laws Second Amendment Act (2008), which clearly states that "no records containing personal information which allows a passenger to be identified shall be retained for longer than necessary for achieving the purpose of Advance Passenger Information processing."[167] In comparison, PNR data is stored for "as long as certain periods require the information to be kept, however certain face value/sensitive information is kept permanently on record."[168] This raises a number of privacy concerns including that the South African government's failure to set strict data retention periods could provide the government with bulk access to PNR data for data mining and profiling purposes, and for mass surveillance.[169]

When comparing the South African PNR regime to the EU standard, South Africa is lacking in terms of the data retention period. The EU found that Canada's PNR retention period of 5 years exceeded what was necessary.[170] To this end, PNR retention should be kept to a minimum time period that is adequate to fulfill the procedures and purpose of PNRs. There is no doubt that South Africa's policy of storing data "[f]or as long as certain periods require the information to be kept" noting that, "certain face value/sensitive information is kept permanently on record" is excessive by international standards and is beyond a reasonable expectation of what should be considered necessary in most circumstances.[171] Neither the South African POPI Act nor the 'new' Immigration Act of 2014 provide restrictions on the retention period of data, clearly contrary to EU standards of data protection.

6.8. *Domestic sharing*

Both the ICAO and the EU state that sharing of PNR data should be limited even in domestic circumstances. Further, the ICAO PNR guidelines note that a "State should ensure that each public authority with access to PNR data provide an appropriate level of data management and protection".[172] Similarly, the EU, in reference to the transfer of PNR data to other government authorities, clearly states that PNR should only be shared and disclosed to other government authorities who are relevant to terrorism and serious crime investigations, that uphold similar standards as the agency that originally received the PNR data, and that PNR data should never be transferred in bulk but only on a case-by-case basis.[173] However, it is important to note that in the US-EU PNR Agreement, the domestic transfer of such data is not limited exclusively to data related to crime or terrorism.[174] Regardless, in South Africa, neither the POPI Act nor any other legal authority, provide sufficient guidelines related to the transfer of personal data within the republic of South Africa.

Given that there is no indication that the domestic transfer of PNR data is restricted or monitored in South Africa, it is difficult to adequately assess the domestic sharing of PNR data in the country. It can be presumed that PNR data is, like APP data, shared with at least: the State Security Agency (SSA), the South African Revenue Service (SARS) and the South African

[160] The Author has requested this a number of times (originally requested in 2017), and has of December 2020, not a single request has been acknowledged.
[161] US-EU Agreement, Article 11.
[162] Amberhawk Training Limited, A review of some important aspects of the EU-USA PNR agreement, 2011.
[163] Enerstvedt, "Russian PNR System", 36-37.
[164] US-EU Agreement, Article 8.
[165] US-EU Agreement, Article 8.
[166] Ibid., 8(5).
[167] Government Gazette 31782, January 8, 2009 [South Africa], http://www.saflii.org/za/legis/num_act/rlsaa2008289.txt.
[168] Email message to the author, January 31, 2018.
[169] Korff, *Passenger Name Records*.
[170] EU-Canada Opinion 1/15.
[171] South African Customs, Email message to the author, January 24, 2019.
[172] ICAO, *PNR Guidelines*, 2.12.1.
[173] Cf. EU Directive, EU- Canada Opinion 1/15.
[174] Article 16.

Police Service (SAPS).[175] However, because PNR data is currently used for border management purposes, the data may be shared with up to the 22 different agencies that are involved in the management of South African borders, including the government agencies who share the task of border protection and security.[176] Without clearly defined practices regarding South African PNR domestic transfer, it is impossible to make a judgment regarding South Africa's domestic PNR sharing. However, given the current status of South Africa's border management, and lack of clear laws to limit the domestic sharing of personal information used for security purposes, it could be suggested that South Africa's practices fall short of international standards.

6.9. *Third country data sharing*

The EU PNR standard clearly restricts the transfer of PNR data to third countries; however, there are some exceptions. The EU standard and the POPI Act share similar principles in that they both limit the transfer of personal information to third countries unless they are deemed to have adequate levels of data protection and the transfer of data is considered to be necessary.[177] Interestingly, even though the EU has implemented the GDPR, the 2016/681 Agreement between the EU and US on the transfer PNR data[178] falls short of the European standard, yet it remains in force.[179] The US-EU PNR Agreement remains somewhat imprecise with respect to third party data transfer. For example, the agreement does not clearly restrict the sharing of data to only that which is related to terrorism or serious transnational crime, nor does it provide restrictions on third country onward transfer of the data.[180] Despite the fact that the GDPR is extraterritorial in that it protects the data of EU residents even if the data is located outside of the EU, the collection and sharing of PNR data is complex because of the many actors and multiple jurisdictions that may be involved. Notwithstanding, while data transfer agreements between the EU and third countries remain limited, there may be occasions where the sharing of PNR data is in the best interest of the EU and third countries.

As previously mentioned, even under the POPI Act, international transfers are permitted as long as the country to which the data is being transferred is determined to have laws similar to South Africa's as they relate to the transfer of personal information outside of state borders; the subject consents to the transfer (which may take place digitally and without the subject's full awareness); the transfer of the data is deemed necessary; and/or the transfer is of benefit to the subject. However, these conditions are ambiguous, and would justify the transfer of data to most countries under the correct circumstances.

It is important to note that South Africa currently does not have any official agreements related to the transfer of PNR data. This is significant, because many PNR-using countries have, or are in the process of negotiating, formal agreements and acknowledge that data may be shared internationally.[181] However, the transfer of PNR data is generally not limited to formal agreements of PNR transfer and often appears to be transferable to countries with 'adequate' levels of data protection. For example, the European Commission has previously recognized "Andorra, Argentina, Canada (only commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and Japan" as having adequate levels of data protection at the time the GDPR was implemented.[182] Further, in the absence of an adequacy decision made by the European Commission, such is the case for South Africa, data may still be transferred to a third country if the controller or processor provides adequate and appropriate safeguards of the data and there are "enforceable data subject rights and effective legal remedies for data subjects available".[183] While it is difficult to determine to what extent PNR data is being transferred outside of formal agreements, there are legitimate channels for countries to facilitate legal transfer of PNR in lieu of such agreements.

The US-EU PNR Agreement on the transfer of PNR data opens space for the transfer of PNR data to third countries. The Agreement between the EU and US, when speaking directly to onward transfer, is relatively vague and only limits the transfer of PNR data to third countries to be "consistent with [the] Agreement", but does not restrict this transfer to only matters of terrorism or serious crime.[184] Further, privacy protection is not necessarily applicable under emergency circumstances.[185] What is most notable in the agreement is that there is no clear requirement to disclose the transfer of data, record the transfer of data, nor is there clear oversight on third party use.[186] Similarly, the EU PNR Directive which applies to EU member states permits the transfer of PNR data to third countries if the receiving body has adequate data protec-

[175] Department of Home Affairs, "Presentation To The Portfolio Committee".
[176] Border Control Operational Coordinating Committee (BCOCC), "Welcome to South Africa Borders," South African Borders, accessed March 15, 2018, http://www.borders.sars.gov.za/Documents/BCOCC-Welcome.pdf.
[177] GDPR Chapter 5 cf. Recital 114, and POPI act Chapter 9(72).
[178] Article 96 GDPR states that "International agreements involving the transfer of personal data to third countries or international organisations which were concluded by Member States prior to 24 May 2016, and which comply with Union law as applicable prior to that date, shall remain in force until amended, replaced or revoked". Given that the US-EU PNR Agreement of 2012 is still in force, it seems likely that there will be renegotiations.
[179] Cedric Ryngaert and Mistale Taylor. "The GDPR as Global Data Protection Regulation?" *The American Journal of International Law* 114 (2020): 5-9.
[180] Amberhawk, *EU-USA PNR agreement* .cf. Enerstvedt, "Russian PNR System", 38.
[181] Cf. Countries that have formal agreements on the transfer of PNR data include Canada, the United States, Europe, Australia, and Japan (in negotiation).
[182] European Commission. "Adequacy Decisions: How the EU determines if a non-EU country has an adequate level of data protection." *Official website of the European Union*. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en#:~:text=The%20European%20Commission%20has%20so,are%20ongoing%20with%20South%20Korea.
[183] GDPR Article 46(1).
[184] US-EU Article 17.
[185] US-EU Article 17(2).
[186] Ibid. Article 17.

tion[187] and is responsible for conducting the prevention, detention, or investigation of a serious crime that the PNR data is required to facilitate.[188] Further, this transfer of data may take place without consent under the condition that there is an immediate serious threat and consent cannot be provided in a timely matter respective to the threat.[189] While the GDPR applies to PNR data, it does not affect the validity of pre-existing international agreements that member states may be party to.[190]

While there is convincing evidence that South Africa shares personal data, once again, there is no information on standards, limitations, or official processes. This implies that it is not only third parties that should be of concern in relation to data protection, but also the South African government itself. It is important to note that the South African government has been moving towards cross border cooperation in terms of information sharing and data management with neighbouring countries.[191] South Africa already has a share border initiative with some countries and has begun to cooperate in a system where "the South African Defense Force will collaborate with Botswana Police, or Botswana Defense Force across the border, to make border control operations more effective, to access information" with the intention of having permanent external–internal liaison.[192] Further, as part of the Southern African Development Community (SADC), South Africa and member states have been working towards harmonization of data protection since 2012[193] in order to guarantee that all members have an adequate standard of protection of personal data.[194] This will allow for legitimate sharing of data among SADC states and clearly shows that South Africa has the intention to share data related to border security with other African states. What remains unclear, however, is whether PNR data is included in these initiatives or to what extent it may be protected.

Currently, South Africa does not have any formal international agreements specifically about the transfer of PNR data, however, the country is party to a number of Mutual Legal Assistance Treaties (MLATs). MLATs are noteworthy in the cross-border sharing of data because they are an agreement between two or more countries, and they create obligations under international law which may include the transfer of PNR data. These obligations imply that governments must provide assistance to each other in criminal matters; as such, "law enforcement officers or prosecutors use them when they need help to obtain evidence from within another country's jurisdiction."[195] Thus, even without formal PNR sharing agreements, MLATS can provide a legal basis for such a data transfer. South Africa currently has MLATs with Argentina, Canada, Lesotho, Egypt, Algeria (not in force), Nigeria (not in force), France, China, the USA, and India[196] – but it does not have any multilateral, regional, or country-to-region MLAT agreements.

The MLAT between South Africa and the USA is interesting because while both countries have ambitious PNR programs, both have also been criticized for their weak protection of personal data.[197] The MLAT between South Africa and the US is particularly important because the US was previously considered as having adequate data protection by both South Africa and the EU, but under the POPI Act (2013) it would no longer be considered to meet the requirements for data transfer.[198] In this case the transfer of personal information from South Africa to the US would have to rely on other protections and or justification. Interestingly, the MLAT would provide a means to make the transfer of PNR data to the USA lawful whereas it would not have been so identified under other authorities/legislation. Simply, it is important to note that under South African law it is possible to transfer PNR data without a formal PNR agreement and in circumstances which may not meet POPI standards.

South Africa is also part of the Kilowatt Group (1977) which is composed of EU Member States, the USA, Canada, Norway, Israel, and Switzerland, and ensures free flow of intelligence about terrorists and extremists.[199] This group is concerned with intelligence exchanges and digitally connected databases and registers; however, the current operational status of this group remains ambiguous.[200] While South Africa's transnational sharing of PNR data remains enigmatic, revelations suggest that data, and possibly PNR data, is being shared internationally, as would be expected from a member of the group: intelligence leaks have confirmed that South Africa has had secret correspondence with the CIA (US), MI6 (UK), Mossad (Israel), FSB (Russia), Iran and more than a dozen other agencies in Africa, Asia, and the Middle East.[201]

---

[187] Builds off of the old 2008/977 Decision, Article 13.
[188] Directive (EU) Article 11.
[189] Ibid.
[190] GDPR Article 96.
[191] Matthew Longo, *Co-Bordering, Cosmopolitanism and the Specter of Empire*, Chapter 4 . In "The Politics of Borders: Sovereignty, Security, and the Citizen after 9/11, 110–36. Problems of International Politics". Cambridge: Cambridge University Press, 2017. 117-118.
[192] Ibid:118.
[193] International Telecommunication Union (ITU) HIPSSA Project (Harmonization of the ICT Policies in Sub-Saharan Africa) Data Protection: Southern African Development Community (SADC) Model Law, ITU. 2013. https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_data_protection.pdf.
[194] Roos, *Data Protection Law in South Africa*, 223.
[195] Access Now, "The urgent need for MLAT reform," Mutual Legal Assistance Treaties, https://www.mlat.info/faq.
[196] Department of Justice and Constitutional Development [South Africa], "Extradition and Mutual Legal Assistance," The DoJ&CD, accessed March 16, 2018, http://www.justice.gov.za/ilr/mla.html.
[197] This is reflective in the fact that the US does not meet South African POPI law standards on the transfer of personal information. Cf. Cf. John Giles, "POPI Update: Parliament Wants POPIA to Commence Urgently" and John Giles, "UN Concerned about Privacy and Interception in South Africa."
[198] Michalsons, "Transfers of Personal Information Outside South Africa," December 7, 2017 https://www.michalsons.com/focus-areas/privacy-and-data-protection/transfers-of-personalinformation-outside-South-Africa.
[199] Stéphane Lefebvre, "The Difficulties and Dilemmas of International Intelligence Cooperation," *International Journal of Intelligence and CounterIntelligence* 16, no. 4 (2003): 531, https://doi.org/10.1080/716100467
[200] Ibid.
[201] AlJazeera Investigative, "The Spy Cables: A Glimpse into the World of Espionage," News | Al Jazeera, February 23, 2015,

From a data protection perspective, the ambiguous situation in South Africa complicates the interpretation of its PNR use, particularly because a PNR is indiscriminate of nationality and should be protected by both national and international law. For example, Enerstvedt notes that international law on data protection includes the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and United Nations Guidelines Concerning Computerized Personal Data Files, among others.[202] Simply stated, until South Africa publicly clarifies its use of PNR there can be no certainty whether or not South African PNR practices reflect international laws and standards.[203]

7. Conclusion

South Africa was one of the most internally surveilled countries in the world during its apartheid era.[204] In fact, the availability of personal data helped the government uphold and facilitate its apartheid regime and was necessary for a continued apartheid state. Then as now, the South African surveillance system was characterized internationally by its non-transparency, excessiveness, and weak legal protections. As a result, the UN and other governmental and nongovernmental actors called on the country to reform its surveillance practices.[205] These reforms were to focus on the right to privacy, protection of data, transparency, and oversight; however, all of these issues continue to plague the country's PNR regime. Noting that the capacity for state surveillance is determined by a country's resources, political will, budget constraints, and geographic restrictions, it ought to be considered that, given the inherent lack of transparency surrounding PNR use in South Africa, the country may not be willing or may not be able to provide adequate measures to protect its PNR data.

Notwithstanding, South Africa's use of PNRs represents the inclusion of an African country in what remains a predominately North American and European practice. In examining the country's PNR regime, it becomes clear that their data management practices have significant implications on the fundamental rights of individuals, although the extent of this, especially as it relates to data protection and data transfer, cannot be confirmed because the government remains unwilling to formally share this information. The excessive PNR practices - due to the failure of the government to specify the purpose of collection, means of use, and because of the potentially permanent retention of data - can be attributed to the equally ambiguous state of its national security services, which are increasingly becoming the watchdogs of society; the State Security Minister recently stated that they "are monitoring everything" in the country.[206] Although some effort has been made in terms of data protection with the implementation of the POPI Act which seeks to bring the protection of personal data in line with international standards, there remains a significant absence of enforcement mechanisms that would align South Africa's privacy protection with international standards and obligations.[207]

The PNR regime in South Africa appears to be based on international standards, but the country falls short in terms of data protection. There remains no clear information related to internal or external transfer of the data and there is little insight into regulatory supervision or accountability; specifically, in light of the many departments that participate in the management of borders. Furthermore, access to information related to PNR and an individual's right to access this information remains restricted. The result of this is that the use of PNR and the lack of information about it suggests that security practices and actors are separated from constitutional and democratic order in South Africa; the use of PNRs for national security purposes has affected the fundamental rights of individuals in that the collection, storage, and potential transfer of PNR data goes beyond any reasonable risk of terrorism or serious crime in the country.

As the first country on the African continent to implement an integrated PNR regime, South Africa's model needs to be given more attention as PNR use becomes a global practice. It is no longer just North American and European states that are using or planning to use PNR for security purposes. As the ICAO and IATA recommendations remain non-obligatory, examination of the South African regime provides insight into the challenges that more countries will face in the implementation of a PNR regime for national security purposes with respect to data protection and privacy.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgement

The author would like to thank Doctor Didier Bigo for his guidance and support throughout the original stages of the research.

https://www.aljazeera.com/news/2015/02/spy-cables-world-espionage-snowden-guardian-mi6-cia-ssamossad-iran-southafrica-leak-150218100147229.html

[202] Enerstvedt,"Russian PNR System", 29.

[203] Ibid.

[204] Dale T. McKinley, "Op-Ed: Is Our Privacy all but Gone?" Daily Maverick, January 30, 2017, https://www.dailymaverick.co.za/article/2017-01-30-op-ed-is-our-privacy-all-but-gone/#.WqI7JpPwbVo.

[205] Privacy International, "UN Calls On Namibia, New Zealand, Rwanda, South Africa, and Sweden to Reform Surveillance. Will the Governments Act?" Privacyinternational.org, March 31, 2016, https://privacyinternational.org/blog/661/un-calls-namibia-new-zealand-rwanda-south-africa-and-sweden-reformsurveillance-will.

[206] Jan Gerber, "We Are Monitoring Everything – Spy Minister Mahlobo," News24: Breaking News. First, May 15, 2017, https://www.news24.com/SouthAfrica/News/we-are-monitoring-everything-spy-minister-mahlobo-20170516

[207] Cole et al, *Surveillance*, 135.