SEAMLESS TRAVELLER JOURNEY

WTTC DISCUSSION PAPER:

DATA FACILITATION - Privacy perspective

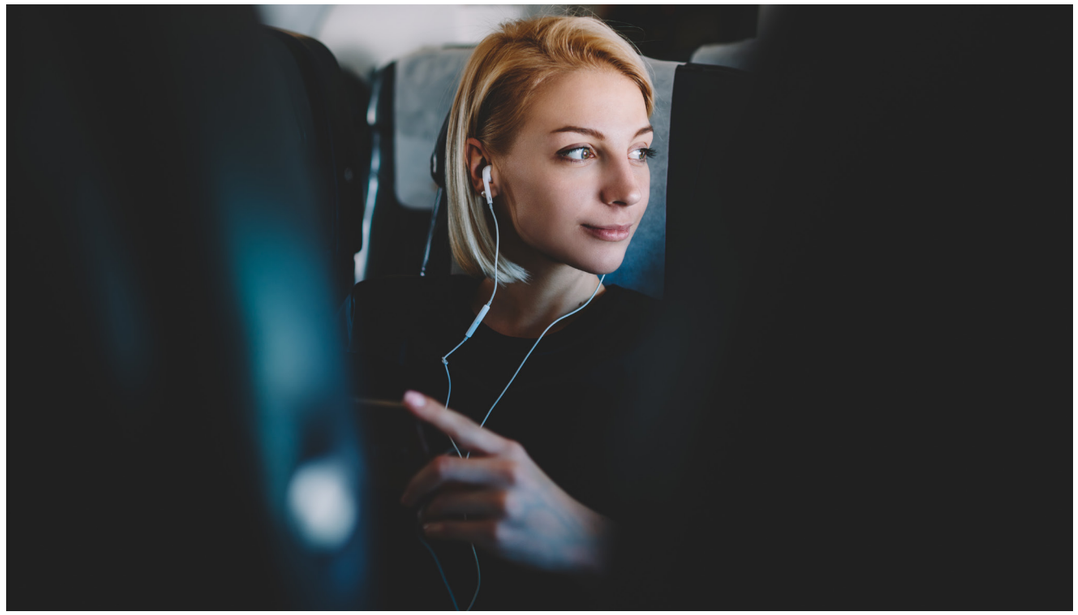
WORLD TRAVEL & TOURISM COUNCIL

CONSIDERATI

OLIVER WYMAN

DATA COLLECTED IN Q3 2019

AUGUST 2020



1. INITIATIVE OVERVIEW

The challenge

WTTC's latest annual research, in conjunction with Oxford Economics, shows the Travel & Tourism sector experienced 3.5% growth in 2019, outpacing that of the global economy (2.5%) for the ninth consecutive year. Over the past five years, one in four new jobs were created by the sector, making Travel & Tourism the best partner for governments to generate employment.

The industry has long tried to improve security, reduce fraud, and improve the traveller experience. Seamless Traveller solutions enabled through biometrics, provide the mechanism to increase security while enhancing the traveller experience across the air and non-air touchpoints. Additionally, contactless biometric technology can assist in the prevention of pathogens' transmission between passengers.

The opportunity

Significant technological advances in digital identities continue to enter the marketplace. These technologies enable verified digital identities that use biometrics to confirm, with high certainty, the identity of a user. Applying these solutions to the Travel and Tourism industry offer significant benefits. Verified identities will enable the secure, seamless movement and management of travellers across the air and non-air journeys. Utilizing traveller biographic, biometric, loyalty, credit card, travel history, proof of immunity or vaccine and other personal information will allow governments and travel providers to more efficiently and safely move the traveller through journey touchpoints. Travellers will no longer be required to present and verify their identity and relevant travel (e.g. recently visited countries) and medical history (e.g. vaccine) at multiple touchpoints. The result reduces fraud and allows for the movement of more travellers securely and efficiently through existing infrastructure and easing resource requirements.

WTTC approach

WTTC defined its global vision for the Seamless Traveller Journey (STJ) as enabling a seamless, safe and secure end-to-end traveller journey encompassing both air and non-air traveller touchpoints. Systematic biometric verified identification at each stage of the journey will replace today's manual identity verifications. These solutions will capitalize on several opportunities including improving the customer experience, creating a frictionless experience at touchpoints, improving security, health safety, and promoting commercial benefits to travel providers. Significant technological advances, especially in biometrics, have enabled digital identity solutions which are demonstrating strong opportunities to enable verified identities. These verified identities enable the secure, seamless movement and management of travellers across travellers' air and non-air journey.

2. LATEST PERSPECTIVE: DATA FACILITATION METHODS

Introduction

The WTTC DISCUSSION PAPER: DATA FACILITATION FOR THE SEAMLESS TRAVELLER JOURNEY provides an update on the progress of WTTC's STJ initiative and discusses three Data Facilitation Methods.
Please visit wttc.org/Initiatives/Security-Travel-Facilitation for the full report.

Several biometric driven solutions are currently operational around the world. While there have been significant benefits realized in each program, overwhelmingly these solutions have been siloed. Limited interoperability across today's solutions present the critical need for global best practices to govern information storage, exchange, and partnership across organizations.

Significant learnings are becoming available from those operational solutions. Taking lessons learned and synthesizing them into standardised approaches to more easily facilitate interoperability is critical to success.

Principles of success

The industry is at a critical point where biometric digital identity solutions are being designed and developed to serve travellers across the air and non-air touchpoints. The proposed facilitation methods start to define models which facilitate the conversation to answer key questions the industry needs to consider as best practices are developed. These questions align with our four principles of success. This paper addresses the Data privacy principle.

1

Interoperability

Scalable solutions seamlessly interact between the private and public sector.
Key open questions:

- How will the industry ensure solutions seamlessly interact across parties within the public and private sector?
- What data standards and requirements will be used to scale solutions across the globe?

2

Data collection and sharing

Data shared in a fully transparent manner with minimum data required, including 'zero-knowledge proof messages' where a traveller provider is given proof data exists without receiving the sensitive information.

Key open questions:

- Who owns the data?
- Where and how will traveller data be stored?
- Who will control the right to share traveller data?
- How is traveller consent shared?

3

Data privacy

Highest standards of data privacy, clear transparency to the traveller and only share operationally required data to travel providers.

Key open question:

- As regulators and travellers mature their stance on data privacy, how are solutions developed to meet today's laws, while being flexible to adapt to future regulation and consumer demands?

4

Intergovernmental and private sector cooperation

Bilateral data sharing agreements between multiple governments and between the public and private sector.

Key open questions:

- How will data sharing agreements between governments be established and how will those government entities work with the private sector?
- How will consent be received from the traveller for the sharing of their data?

3. DATA FACILITATION METHODS OVERVIEW

As scope expanded to include air and non-air travel, two emerging models became the backbone of the biometric traveller journey. (1) Per Trip, allows a traveller to create a single journey token in advance via mobile device or in-person at check-in. Following their trip, the token containing the traveller data is purged. (2) Per Life, where travellers enrol once to create a verified digital identity which exists until the traveller decides to purge their digital identity. Government has become a data facilitation method which can facilitate both, the Per Life and Per Trip models.

To enable the Per Trip and Per Life model, traveller data will be stored and shared across multiple stakeholders in the traveller's journey. We have defined three data facilitation methods to enable this:

1. **Centralised**: traveller data is stored and managed on a central platform which travel providers must connect.
2. **Decentralised**: traveller data is stored on their mobile device and pushed to travel providers by the traveller.
3. **Hybrid**: uses both centralised and decentralised methods within a single traveller journey.

FACILITATION TYPE	DESCRIPTION	EXAMPLE
CENTRALISED	1. Traveller data is centrally stored and managed by a 3rd party 2. Travel providers connect via secure API connections 3. Two centralised providers: • **Private Corporation:** Traveller actively enrols their digital identity data which is stored by a 3rd party provider • **Government:** Traveller biographic and biometric (optional) data collected through government issued documents (e.g. passport, eVisa, etc.)	**Private Corporation:** Clear in the United States **Government:** United Arab Emirates uses Smart Gates at certain points of immigration.
DECENTRALISED	1. Digital identity data owned and managed by the traveller and stored in a digital wallet on their mobile device 2. Traveller manages the data that is pushed to chosen stakeholders and when it is sent	Apple Pay, where user manages their information which lives securely on their personal device. At the time of purchase, a user determines when and where to share their information
HYBRID	1. Utilization of multiple technologies and/or facilitation type across stakeholder systems throughout the travel value chain 2. Processes for integration not yet designed, so many options may exist	

In today's environment, centralised is the most prominent data storage and facilitation method for biometric driven travel programs. Centralised platforms align with traditional strategies where consumers provide large institutions with personal data and each company owns and manages that data in exchange for customers receiving benefits. But consumers stance on data sharing, transparency, and control is shifting.

Consumers are beginning to demand greater control and transparency of their data. The fundamentals of the decentralized data storage and facilitation method account for this shift, allowing travellers ownership and transparency over how their data is used and shared. However, the reality is certain institutions, such as governments, will always have some form of centralised data facilitation. A government views the data of their citizens and those visiting paramount to national security and will, therefore, maintain ownership and management of their data. Since government validation of identity will always be a critical component of a travellers journey, the reality is end-state solutions will need to support a hybrid of centralised and decentralised.

4. INTRODUCTION TO GDPR AS IT RELATES TO THE SEAMLESS TRAVELLER JOURNEY

Technology and data create opportunities for every organization. However, attention to legal, ethical and societal aspects has become indispensable for successful innovations. The growing attention in the media and among policymakers demonstrates this. As an organization, you want to remain in control. The WTTC understands this very well, which is why one of four key principles of the Seamless Traveller Journey Programme (STJ) is 'Data Privacy'.

Nations around the globe have issued or improved privacy legislation as an answer to fast-moving digital innovations. The most prominent, comprehensive, and most strict privacy rules are imposed by the European Union (EU) Regulation 2016/679, better known as the General Data Protection Regulation (GDPR). We will delve into the privacy aspects of STJ, focusing on data sharing and, to a lesser extent, biometric technology. From a GDPR perspective.

General Data Protection Regulation (GDPR) Definition

As of May 25th, of 2018, organizations must comply with GDPR. The rules laid down in the GDPR are not necessarily new[1]. However, the GDPR provides authorities with greater supervisory powers and imposes accountability requirements on organizations that process personal data[2]. This means organizations not only have to comply to the GDPR, but they also need to be able to demonstrate it. Failure to abide by these rules will not only harm the rights of those involved, but organizations also risk high fines and reputational damage.

Even though the GDPR is an EU Regulation, its territorial scope reaches beyond EU borders. The GDPR applies to organizations established within the EU or the European Economic Area (EEA), regardless of whether their data processing activities take place within those borders. The GDPR also applies to organizations outside of the EU or EEA that offer goods or services to - or monitor the behavior of EU residents. This means the GDPR applies to many organizations, especially within a travel and tourism context. For example, a branch of a Germany-based airline that operates solely in Asia, would still have to adhere to the GDPR. Also, it is not unthinkable that U.S. airports would have to comply with the GDPR, depending on whether they target EU residents with their services.

Principles and rationale of the GDPR

For an organization to legitimately process personal data it is important to first have a purpose for the processing activity. The processing activity should be necessary to achieve the intended purpose. Secondly, one of six legal bases to process personal data should be applicable. These legal bases are:

a. Consent.

b. Necessary for the performance of a contract (e.g. certain information is necessary in order to book a flight or a hotel room).

c. Necessary for compliance with a legal obligation (e.g. tax obligations).

d. Necessary for a vital interest of the person in question (almost exclusively applicable in life or death situations).

e. Necessary for the performance of a task in the public interest (e.g. law enforcement or border control).

f. Necessary for a legitimate interest (e.g. security or some types of marketing).

After successfully identifying a purpose and legal basis, the processing activity is most likely to be legitimate. However, there are many other requirements to fulfill to process the personal data responsibly. An exhaustive list of these requirements goes beyond the scope of this article, but think about transparency, data management and data security requirements.

1. Before the GDPR there was the EU Directive 95/46/EC, also known as the Privacy Directive.
2. Personal data is any information relating to an identified or identifiable natural person.

5. PRIVACY IN THE CONTEXT OF THE SEAMLESS TRAVELLER JOURNEY

Biometric data for the purpose of uniquely identifying a person

One of the pillars of STJ is the use of biometric technology, more specifically facial recognition. The GDPR prohibits processing of biometric data for the purpose of uniquely identifying a person, unless one of the exceptions applies.

The only relevant exceptions in the context of STJ are either:

- Explicit consent by the user; or
- Whenever the processing of biometric data is necessary for reasons of substantial public interest.

The former is the only possible exception for private organizations. The latter is a possible exception for public organizations, depending on the context. For instance, biometric technology could be necessary for substantial public interests relating to border control.

Data sharing

Another important aspect of STJ is data sharing. It would be detrimental for a 'seamless' travel journey if travelers repeatedly have to share their data with the next partner whenever they enter the next step in their journey. It is important to note that both the data receiving party as the data sharing party need to have a purpose and a legal basis for the data transfer. In the context of STJ that legal basis would most likely be consent of the user.

In the case of cross-border data sharing, it is important to be aware of differing legal regimes in both countries. Within the EU there is, for the most part, harmonization of privacy legislation through the GDPR. However, outside of EU/EEA borders other – less strict - standards may apply. Some countries have received an adequacy decision from the European Commission, meaning they are considered to have a similar high standard of data protection, such as Canada, Argentina, Japan and Israel. Please note that up until July 16th of 2020, also organizations in the USA within the EU-US Privacy Shield framework were regarded to have an adequate level of protection of privacy, however, the Court of Justice of the European Union has invalidated Privacy Shield in their groundbreaking decision in the Schrems II case. For cross-border data transfers (from within EU/EEA to outside of those borders) to be legitimate, an adequacy decision or additional contractual safeguards (standard contractual clauses, provided by the European Commission) should be in place, among other more complex options.

6. ANALYSIS OF THE SEAMLESS TRAVELLER JOURNEY MODELS

WTTC have defined three facilitation options: centralized, decentralized and hybrid. With each facilitation option come different legal challenges and privacy risks, which should be mitigated in different ways. In this chapter, the most important challenges and risks shall be set out for each facilitation option. Please note that this is not an exhaustive list, but merely an overview of the most important or notable challenges and risks.

Centralized

The idea behind the centralized facilitation model is that traveller data shall be centrally stored and managed by one party. This party could be part of the STJ partnership or a third party. In many cases, this party shall be a government body. Because of the multitude of parties involved in the STJ (air carriers, airports, border authorities, hotels, car rentals, cruise lines and more), that all process personal data for different purposes, legal bases and exceptions, it can be a challenge to determine which party is best suited to collect or store the personal data. Another challenge is to determine the best moment and means for requiring and managing consent. Upon requiring consent, (a subset of) the personal data shall be distributed between the relevant involved parties.

Generally, consent is acquired during an enrollment procedure, either on-site on an enrollment kiosk, or remotely through an app or browser. Consent should always be freely given, informed, specific and unambiguous. Considering the plurality of partners a traveller encounters on a traveller journey, but also the complexity of the data processing activities, it can be challenging to provide the traveller with complete yet comprehensible information on which the traveller can base their consent. Moreover, travellers always have the right to revoke their consent. STJ partners not only have an obligation to inform travellers of this right to revoke consent, but the process of revoking consent should be just as easy for the traveller as to grant consent. For instance, if consent can be provided by a mere click of a button, revoking consent cannot require a traveller to log-in to a website, fill in a form, substantiate the reason for revoking consent, and subsequently take days to process before the data are ultimately deleted.

It is important to determine, either jointly or separately, where the controllership, duties and liabilities of one party end and those of another party begin. Arrangements regarding governance, data security and handling data breaches are key, especially regarding centrally storing the data and data in transit.

Lastly, dealing with a multitude of (global) parties can be complex, even for lawyers. Transparency requirements demand travellers be informed about the data processing activity and the parties involved, in a comprehensible way, also if the data processing activity is not based on user consent. Considering the complexity of STJ, this might prove to be a challenge, especially in a global travel and tourism context where travellers come from different places and speak different languages. Therefore, utilizing universally used icons is advised, as well as the use of clear and plain language.

Decentralized

In the decentralized facilitation option, the biometric digital identity of the traveller is stored on their own mobile device. In this model, travellers can choose for themselves which mobile device and provider they like and trust. Effectively providing them with more control over their personal data. However, considering the complexity of STJ, providing more choices for the traveller can be overwhelming. Can it be expected of the traveller to fully understand the consequences of their choices and actions? This is not so much a legal as it is an ethical point. However, organizations do have an obligation to inform their users adequately and intelligibly, in order for them to be able to make an informed decision on whether or not to share their personal data.

Providing travellers with more choices might also mean that data controllers have less choices, for instance when it comes to picking the mobile devices on which the (very sensitive) biometric data is stored. Each and every STJ partner that processes personal data of travellers, whether it is as a data controller or a data processor, still has an obligation to ensure data security for their own data processing activities, which might be problematic considering some mobile devices are more trustworthy than others.

Hybrid

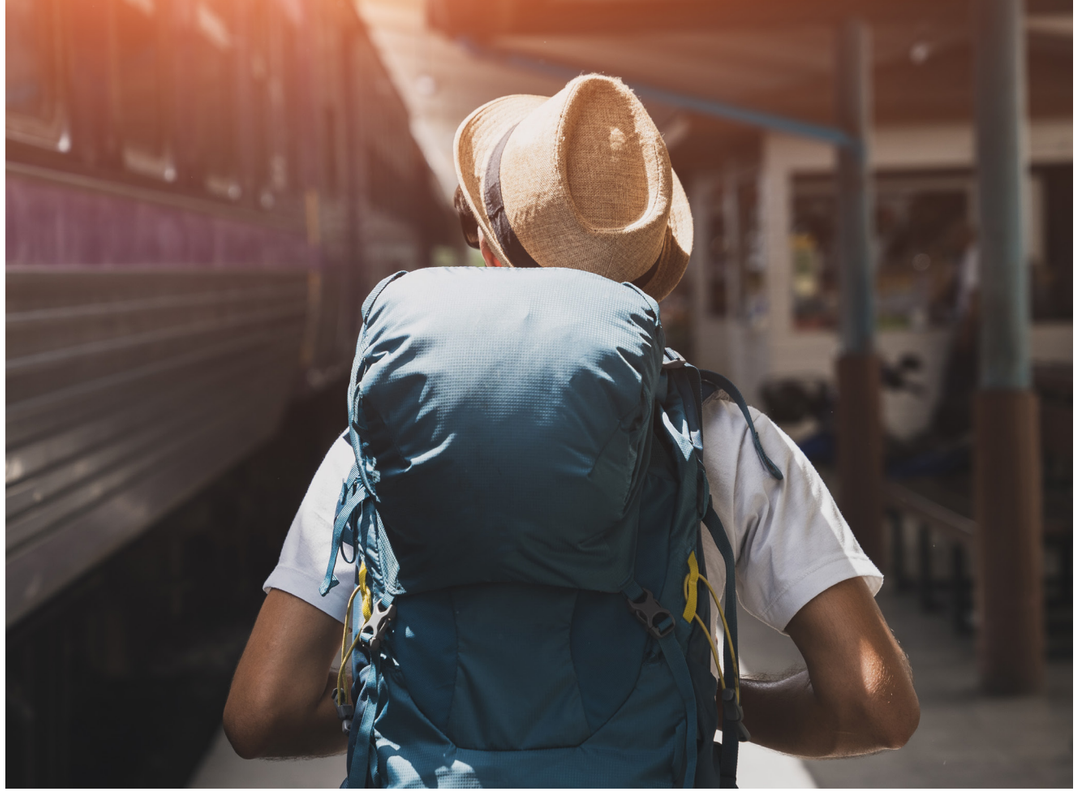
In the hybrid model, multiple technologies or facilitation options are used throughout the travel value chain. As processes for integration are not yet fully developed, the specific challenges paired with the hybrid facilitation option are yet to be determined as well. However, it shall probably be a combination of the aforementioned two facilitation options.

7. CONSIDERATIONS

Seamless Travel Journey will have significant impact on the way the travel and tourism industry develop itself in the near future. The benefits for both travellers and organizations in the travel industry are evident, but so are the privacy risks and challenges involved. There is a great variety of organizations with varying backgrounds and applicable legal regimes, that may deploy the technology for differing purposes and uses. Therefore, a case-by-case assessment of the specific challenges and risks is in order. The best way to assess the legality and to identify the risks and recommended risk mitigating measures of a specific data processing activity, is to perform a Data Protection Impact Assessment (DPIA). In the context of STJ and the aforementioned facilitation options, it is always obligatory to perform a DPIA, under EU law.

Besides performing a DPIA, key points to take into consideration are:

- Processing personal data should be lawful, fair and transparent. Adequately inform travellers about the identity of the involved parties, their purposes, the way they handle and protect the personal data and the travellers' rights.
- Whenever the data processing activity is based on consent, ensuring the consent is freely given, informed, specific and unambiguous. Furthermore, consent should be logged, and revoking consent should be just as easy as providing consent.
- Data security. Both organizational and technical measures should be implemented to safeguard confidentiality, integrity, and availability of personal data.
- Process personal data only for specified, explicit and legitimate purposes and do not process the data for other, incompatible purposes. Do not process more data than is necessary to achieve the intended purposes and ensure the personal data are deleted upon achieving those purposes.



ACKNOWLEDGEMENTS

EDITORS

Jules van Stralendorff LLM CIPM
Legal Consultant | Privacy & Data Protection

In partnership with:

Helena Bononi
Vice-President Membership & Commercial
World Travel & Tourism Council

Lawrence Burka
Associate
Oliver Wyman

For more information, please contact:

Helena Bononi
Vice-President Membership & Commercial
World Travel & Tourism Council
helena.bononi@wttc.org