D9.6: Typology of ethical, legal and societal issues of risk based screening

Document Version 2.0
Document Date: 7 May 2020

Work Package 9: Ethics and Data Protection

Document Dissemination Level: Public

TRESSPASS
robusT Risk basEd Screening and alert System for PASSengers and luggage
is funded by the Horizon 2020 Framework Programme of the EU for Research and Innovation.
Grant Agreement number: 787120 — TRESSPASS — H2020-SEC-2016-2017/H2020-SEC-2016-2017-2

ABSTRACT

The goal of the TRESSPASS project is to develop, demonstrate and validate a single cohesive risk-based border management concept for air, maritime and land border crossing points. As part of this goal, the project follows an Ethics and Data Protection by Design (EDPbD) approach that builds on previous ethical research (Volkmann 2013a, 2017).

In this report, we identify those ethical, legal and societal aspects (ELSAs) that become relevant as *unintended negative effects* of implementing risk based border checks as part of a future border management regime. Twelve types of such ELSA related negative impact have been identified as part of a structured typology that addresses three main categories of ELSAs:

RELEVANT ELSAS FOR RBBM

ELSA category A: Privacy and data protection	ELSA category B: unfair distribution of impact across different social groups	ELSA category C: restrictions of societal freedoms and liberties
Intrusion into spatial privacy	Disproportionate impact due to infeasibility of standard checks	Accosting travelers
Intrusion into bodily privacy	Disproportionate impact due to accumulation of false alarms	Lack of accountability
Intrusion into private life	Disproportionate impact due to false or incomplete external data	Restriction of self-determination and misuse of data
Disclosure of information	Impact on non-travelers	Lack of transparency

This typology will form the basis for an evaluation framework that will be developed as part of deliverables D9.7 and D9.8 (due in M18 and M36). The framework will allow a *comparative assessment* of introducing risk based screening concepts for border checks. It aims at allowing a better understanding *of the positive as well as of the negative effects* of introducing risk-based border checks as part of a future border management regime – and it will do so by comparing the effects of the procedural designs of border crossing points along the twelve types of potential impact specified in the present report's typology.

The types of impact identified in this typology have been conceptualized in such a way to allow the formulation of qualitative scales for assessment. These scales will be used as part of the ethical evaluation framework. By focusing specifically on risk-based approaches, we ultimately aim at enabling designers and decision makers – as well as, to a certain level of detail, the interested public – to evaluate the impact of introducing risk-based border checks. We hope that this will allow ethically informed and well-balanced decisions about the kind of checks at Europe's external borders.

The evaluation framework complements D1.4's analysis of the current legal framework for border checks (which does not allow for risk based approaches), by addressing ELSAs beyond the question of *current legal permissibility*.

Project Information

Project Name	robusT Risk basEd Screening and alert System for PASSengers and luggage
Project Acronym	TRESSPASS
Project Coordinator	National Center for Scientific Research "Demokritos", EL
Project Funded by	European Commission
Under the Programme	Horizon 2020 Secure Societies
Call	H2020-SEC-2016-2017 (SECURITY)
Topic	SEC-15-BES-2017 "Risk-based screening at border crossing"
Funding Instrument	Innovation Action
Grant Agreement No.	787120

Document Information

Document reference	**D9.6**
Document Title	**Typology of ethical, legal and societal issues of risk based screening concepts**
Work Package reference	Task 9.2
Delivery due date	30.11.2018
Actual submission date	
Dissemination Level	Public
Author(s)	**Sebastian Weydner-Volkmann**
Contributor(s)	

Document Version History

Version	Beneficiary	Comments
2.0	ALU-FR	Document revision following review feedback. Minor orthographic corrections and improvements for readability; extended description of the scope in Chapter 1; added references to whitepaper "Ethics in TRESSPASS"

List of Acronyms and Abbreviations

ACRONYM	EXPLANATION
CONOPS	Concept of operations
ECJ	European Court of Justice
EC	European Commission
ELSA	Ethical, legal and societal aspects
EU	European Union
TRESSPASS	robusT Risk basEd Screening and alert System for PASSengers and luggage
BCP	Border Crossing Point
BDPbD	Privacy and Data Protection by Design
PNR	Passenger Name Record

Table of Contents

1 INTRODUCTION

1.1 Background

The goal of TRESSPASS is to develop, demonstrate and validate a single cohesive risk-based border management concept for air, maritime and land border crossing points. This innovation action project addresses border control tasks at regular border crossing points, such as customs and smuggling prevention, immigration control, police searches for suspects, as well as cross border crime and terrorism prevention. Under a newly developed single cohesive concept, related threats will be managed as risks tailored to the specific situational needs of individual border crossing points. The project follows an "ethics and data protection by design" approach that builds on previous ethical research as part of the EU FP7 project XP-DITE.

TRESSPASS will:

(1) Develop a single cohesive risk-based border management concept.
(2) Apply an ethics and data protection "by design" approach.
(3) Include passenger trust in risk management model and perform sensitivity analysis and optimization.
(4) Develop three pivoting pilot demonstrators.
(5) Demonstrate the validity of the single cohesive risk-based border management concept by using red teaming and simulations.
(6) Prepare for the further development of this concept beyond this project by linking to other known risk-based border management projects (in- and outside EU, within EU research frameworks and on national levels), and describe how their results contribute to a single cohesive risk-based border management concept.

1.2 Aim and scope of this document

The aim of this report is to document the identification of ethical, legal and societal aspects (ELSAs) that may become relevant as unintended negative impact of introducing risk based border management. Twelve types of ELSA related negative impact have been identified as part of a structured typology that addresses three main categories of ELSAs:

- ELSA category A: privacy and data protection issues;
- ELSA category B: unfair distribution of impact across different social groups;
- ELSA category C: restrictions of societal freedoms and liberties.

These issues have been conceptualized in such a way as to be compatible to the overall CONOPS framework: Procedural designs of (risk-based) border checks will be evaluated on qualitative scales of assessment from better to worse with regard to each of the issues identified in this typology (e.g. ranging from "hardly any impact" to "very intrusive" regarding travelers' private life). For this, future reports will define a methodological framework that allows a comparative evaluation of different design options.[1] As a first step, the present report provides a situational specification of abstract normative concepts like privacy, non-discrimination or societal liberties with regard to border checks at border crossing points at EU external borders.

[1] This will be documented in deliverables D9.7 (preliminary version, M18) and D9.8 (final version, M36).

The ability to assess the ELSA related impact of different forms of border checks will allow informed decision making as part of the design and policy process: It will provide awareness regarding the ethical trade-offs involved and provide the intellectual tools necessary to make conscious design choices about normative concepts like privacy, data protection, non-discrimination, etc. (Ethics and Data Protection by Design, EDPbD). By focusing on risk-based approaches, we ultimately aim at enabling designers, decision makers, and – to a certain level of detail – the interested public to better understand the *positive as well as the negative effects* of introducing risk-based border checks at the Union's external borders.

The framework will go beyond the scope of deliverable D1.4, which provides a detailed analysis of the current legal framework for border checks. Since the *current* legal framework does not allow for risk based approaches, the outcome of the TRESSPASS project, by definition, addresses a *potential future legal context*, in which we posit that a legal basis for risk-based checks exists. Since we cannot predict the outcome of a corresponding legislative process, our assessment of the ELSA related impact will go beyond questions of current legal permissibility and analyze the impact of risk based border checks along the twelve types of impact identified in the present report.

Please note that research ethical questions are out of scope for this report. Documentation on how the relevant legal and ethical requirements for responsible research are addressed throughout the duration of project is provided in deliverables D9.1 through D9.5. A good starting point for looking into these questions is the first periodic ethical report (D9.3). Annex G of that report also includes an overview over how different aspects of ethics are addressed in TRESSPASS's different work packages and tasks (Whitepaper "Ethics in TRESSPASS).

1.3 Input / Output to this document

- **Input** to this report have been the early conceptual discussions from Work Packages 1 and 2, as well as preliminary work on the overall CONOPS framework from Work Package 6.
- **Output** from this report will be used in a variety of tasks, such as Task T1.4 (Legal and regulatory framework) and Task T2.2 (Risk indicators). In the main part, however, this typology will form the basis for an evaluation framework to be developed as part of deliverables D9.7 and D9.8.

2 BORDER CHECKS, RISK BASED SCREENING AND ETHICS

In this chapter, we will further define the scope of this report and develop our approach towards a typology of ethical, legal and societal issues relevant for risk based border management. Our approach will be similar to the one used in XP-DITE's Ethical Framework (Volkmann 2013a), but it will have to be re-developed with a different area of application in mind, i.e. border checks for travellers (including customs checks) with a specific focus on risk based screening methods.

2.1 The logic of border checks (including customs checks) for travellers

The Schengen Border Code (EU 2016a, Art. 2) defines 'border checks' as one of two main activities that make up 'border control' (governing people's movements across borders): in contrast to 'border surveillance', which deals with enforcing that borders are only crossed at 'border crossing points' (BCPs), 'border checks' refers to "the checks carried out at border crossing points, to ensure that persons, including their means of transport and the objects in their possession, may be authorised to enter the territory of the Member States or authorised to leave it". By including objects in the possession of persons crossing a border, border checks touch on a separately regulated and (in many countries) separately enforced regime, i.e. the customs regime, understood as governing the movement of goods across borders.

As such, the two regimes each follow their own distinct set of goals. An example for such separate goals due to different regimes in place could be, for example, the generation of revenue for the state through taxing certain goods that cross the border (a task from the customs regime) versus preventing that specific persons can enter or leave a certain territory (a task from the border control regime). As part of the process of checking persons who cross a border, however, the two regimes follow essentially the same logic, which follows two main functions: (1) they perform access and egress control in a spatial sense based on (2) information revealed by inspection. We will call the first function 'access and egress control function' and the second 'revelatory function'.[2]

Access and egress control presupposes the idea of a spatial separation – here a territorial separation. Crossing over from one territory to the other is subject to it being officially determined that the regulatory conditions are met; otherwise moving across the border is denied. At a fundamental level, this is a binary decision process with the aim of determining if a traveller (including the goods they bring along) is allowed to move along or is denied to do so (Zurawski 2015, 15–17; Rule 1974).

If access and egress control is to be performed in a meaningful way that helps enforcing the border control and customs regimes, it must be able to deal with situations where travellers deliberately make false claims about their person or about the goods they bring along with them. Hence it is dependent on the revelatory function, which needs to (a) *reveal the identity* of persons and their belongings to border guards or customs officers, so that they can be *subsumed under certain regulatory categories*, which in turn imply different conditions under which they can or cannot move across the border (e.g. 'persons enjoying the right of free

[2] This resembles very closely the two main functions of passenger screening in aviation security as shown in XP-DITE (Volkmann 2013a, 12–13). This resemblance has the benefit of allowing some form of compatibility between the approaches to the evaluation of border checks in TRESSPASS and to that of passenger screening in aviation security in XP-DITE – which has been foreseen in the TRESSPASS project.

movement under Union law' or 'goods made from an endangered and protected species). Furthermore, the revelatory function needs to (b) uncover whether a person's identity has been *deliberately falsified* or the presence of certain goods or other persons *concealed from plain view*. [3]

Within the Schengen Area, border checks at border crossing points are only foreseen at the EU's external border, not at internal borders (EU 2016a, Art. 22) – although temporary border checks are allowed in certain exceptional situations (EU, 2016, Art. 25), as are certain types of police checks that do "not have an effect equivalent to border checks" (EU 2016a, Art. 23). Since bulk cargo is out of scope for TRESSPASS, we can thus further limit the scope of the approach *by conceptualizing border checks as performing the access and egress control function based the revelatory function with regard to the movement of persons and the goods they bring along with them (including the means of transport) at the external borders of the EU.*

2.2 The purpose of performing border checks

As mentioned above, the purpose of performing the two main functions of border checks are governed by different regimes that have different purposes in mind and that are operating in different normative contexts. For example, customs related checks at BCPs may be a way of enforcing that customs duties are payed for importing goods – which, in turn, may be a form of revenue generation for governments, or they can serve as an international policy instrument, e.g. for protecting local industry or for punishing the policies of a foreign government. Furthermore, customs related checks can serve the purpose of preventing that certain goods cross the border without knowledge and clearance of the competent official bodies – in this case, potential tax revenues are ignored for the benefit of different purposes. These range from considerations of public security, e.g. preventing that unregistered firearms are brought into the country, to considerations of protecting endangered species, e.g. preventing that ivory can be imported.

Similarly, border checks at BCPs are conducted for a broad range of purposes, for example, for preventing persons entering a country who cannot sustain the costs of living by themselves and could, consequently, burden a state's social welfare system or else be expected to resort to illicit work or illegal activities. A different purpose for border checks could be security considerations like the protection of public health in case of an epidemic, or preventing perpetrators of serious crime or terrorism from entering or leaving a country.

There is, hence, no singular and consistently specifiable end with regard to border checks (as opposed to, for example, passenger security screening in aviation security). In the abstract, we can define the purpose of performing the two main functions of border checks as allowing the governance of persons who cross the border by enforcing the corresponding regimes. Any concrete form of such enforcement, however, is to be seen in relation to its respective ends.

A further specification is *only tentatively* possible due to the focus of TRESSPASS on risk based border management: because the risk management concept is planned (cf. Task T2.1) to be based on a "Design Basis Threat" specification for each BCP, we expect the most prominent purposes to be "threat related". The Schengen Border Code lists the following threat related purposes with regard to the entry conditions: Third country nationals

[3] For border checks, the revelatory function has a much greater emphasis on *identifying* goods and persons as opposed to aviation security, where *detecting* the presence of specific threat items is at the center.

> *… are not considered to be a threat to public policy, internal security, public health or the international relations of any of the Member States … (EU 2016a, Art. 6 (1) e)*

While for third country nationals, "thorough checks" corresponding to those purposes are mandatory on entry (EU 2016a Art. 8 (3) a vi) and "whenever possible" on exit (EU 2016a Art. 8 (3) g iii), EU nationals and persons enjoying the right of free movement under Union law may also be subject to threat related border check procedures:

> *… on a non-systematic basis … border guards may consult national and European databases in order to ensure that such persons do not represent a genuine, present and sufficiently serious threat to the internal security, public policy, international relations of the Member States or a threat to the public health.*
>
> *The consequences of such consultations shall not jeopardise the right of entry of persons enjoying the right of free movement under Union law into the territory of the Member State concerned … (EU 2016a, Art. 8 (2))*

Of the four threats explicitly mentioned in the Schengen Border Code, i.e. threats to public policy, internal security, public health or the international relations of any of the Member States, only the threat to public health is specified further in the definitory section, by referring to epidemic, infectious, or contagious parasitic diseases so far as Member States have implemented protecting measures against them (EU 2016a, Art. 2). With regard to public policy, internal security and international relations, we are dealing with "indeterminate legal concepts" that cannot be read as continuous with the national legal concepts – similarly to the concept of free movement of goods (Grabitz, Hilf, and Nettesheim 2018, AEUV Art. 36 Rn. 17-21, my translation). They allow a relatively broad interpretation to be specified in the legal and socio-political context of the Member States. Furthermore, these concepts "open up" the Union's border check regime to measures regarding law enforcement, crime prevention and emergency response at the border, e.g. with regard to the search for fugitives of the law through national and EU databases, the identification of suspected terrorist or of persons involved in organized crime, or preventive measures against a spreading epidemic.

Depending on the specific measures, further EU legislation may be involved and, through that, further specification of the purposes pertinent to those measures may be specified. For example, the collection and processing of passenger name record (PNR) data is regulated in Directive (EU) 2016/681. In that regulation, the measure of PNR data processing is bound to threat related purpose of fighting (preventing, detecting, investigating and prosecuting) terrorist offences and serious crime. Consequently, processing PNR data is not allowed, for example, for purposes of protecting endangered species (e.g. by assessing which passengers may be involved in smuggling ivory).

2.3 Identifying relevant ELSAs of border checks

The term 'ethical, legal and societal aspects' refers to a wide field of different forms of social values; some of those values govern the purposes of border checks (and hence inform the corresponding legal regimes), others become relevant because of the ways we try to attain these purposes. The first type of norms correspond to intended consequences of border checks, the second type to unintended consequences (be they good or bad). When we try to identify relevant ELSAs in addition to the purposes that govern border checks at BCPs, we imply that, even if we deem those purposes legitimate, there may still be a range of conflicting values that should be considered when we evaluate the specific procedures implemented at BCPs.

To a certain degree, the importance of considering unintended consequences is reflected in the different legal regimes that govern border checks. For example, the regulations limit the power of border guards in favour of other, potentially conflicting values – like the protection of privacy or the prohibition of discrimination. Nevertheless, these legal regimes also operate in a wider normative context that needs to be considered. Even if we assume that a certain activity by a border guard has, in general, a clear basis in the law and is also legally permissible in that situation (because it is deemed proportionate, necessary and appropriate for attaining a legitimate purpose), then this does not mean that there are no further collisions of values to be considered. It only means that for dealing with potential normative conflicts, we can *make use of institutionalized rules and processes*, i.e. of the regulatory provisions and, if necessary, of the legal ways to challenge and change them. But dealing with conflicting norms by referring to the legality of an action does not 'resolve' the conflict in the sense that it suddenly ceases to exists or that all conflicting values suddenly align neatly in such a way that, once you solve the legal issues, you can expect to have solved all other normative issues as well.

Hence, for identifying not only legal, but also ethical and societal aspects of border checks, we cannot simply look at what is legally permissible and what is not. Rather, we have to consider a much wider horizon of commonly shared social values within Europe and identify those that are relevant for evaluating border checks. This is underscored by the fact that, since we can arrange border checks in different ways, this will also have different unintended consequences vis à vis these values. Therefore, answering the binary question of legal permissibility will not help us to actively minimize unintended negative consequences of border checks. Instead, our approach to identifying all ethical, legal and societal values that become relevant for the evaluation of border check procedures will start from considering which values may come into conflict with the logic of border checks outlined above.[4]

As a first set of conflicting values, we can already identify norms of privacy and data protection: Since, in order to attain their purpose, border checks always have to reveal information about persons or their belongings that are not already publicly visible or divulged voluntarily (i.e. information that is private), it lies in the nature of border checks to necessarily come into conflict with privacy related values. Because border checks also make use of automated data processing, this includes aspects of data protection (in so far as personal data is processed). This can serve as an example to illustrate that, even if we consider certain forms of border checks *legally permissible*, the impact with regard to norms of privacy and data protection will persist: bags of travelers will still be opened to reveal their contents, or biometric data will still be processed to verify a traveler's identity.

While legal permissibility can be used to *justify* such impact, further and more deeply rooted evaluations are possible by better understanding the nature of this impact in the light of ethical and societal norms that inform the current legal provisions. By not restricting our understanding of the relevant ethical and societal norms to how the current legal doctrine incorporates them, we can then move to a broader historically and culturally informed

[4] In TRESSPASS Deliverable D1.4, the current legal framework for border checks is analyzed to identify what changes would be necessary to allow for risk-based border management. Since, currently, the regulation doesn't provide a clear basis in the law for risk based border management, TRESSPASS (by definition) addresses a potential *future* legal context, in which we posit that such a legal basis exists. Again, this highlights the need for an analysis of ethical, legal and societal aspects beyond questions of legal permissibility, since we have no way of predicting how such a legal basis would turn out. To the contrary, a wider consideration of shared values can then be used to inform future political and legislative debates around what of checks *should* be permissible at the EU's external borders.

perspective on those values. In doing so, we reflect on the normative context of our experience with respect to different implementations of the two main functions of border checks.

Determining the relevancy of values to our inquiry by relating them to the two main functions of border checks means that many normative aspects will move out of the focus of our analysis – despite being ethically relevant in their own way: For example, the revelatory function is formulated too narrow in order to cover ethical questions that have to do with the *physical impact* on the body of the traveler who is subject to screening. This means that the two main functions of border checks will not shed light on questions regarding health and safety aspects. Furthermore, since the two main functions scrutinize the *effects on the traveler*, the impact on the border guards conducting the checks and the conditions under which they work moves out of the center of attention.

These 'blinders' of the approach help us to limit the scope of our theoretical approach; they act as what John Dewey (1981, 25) called "deliberate omission, for the purpose of the inquiry in hand", i.e. they help us focus on the specific problems to be addressed. For example, ethical and societal questions regarding the fair pay of customs staff are quite relevant in their own respect, but they are not directly related to the purposes of border checks, nor to the procedural activities and technologies used in these checks – they are not *typical* issues of border checks (cf. section 2.5 below), nor of TRESSPASS's focus on risk based border checks.

2.4 Risk-based border checks and ELSAs

Not unlike risk based passenger screening in aviation security (cf. Weydner-Volkmann 2017, 2018, 154–75), the introduction of risk based border management is a modification of *how* the purposes of border checks are to be attained, i.e. it is a modification of the ways in which the two main functions of border checks are meant to be applied. Although a risk based approaches alter the *ways* in which border guards deal with different forms of threats, they don't, by themselves, introduce wholly new, separate purposes of border checks and they don't change the fundamental logic of border checks, which was outlined in section 2.1 above (revelatory function, access and egress control).

Risk-based border management, thus, implies a certain type of arrangement of the border and customs check procedures. As mentioned above, different arrangements will not only have different *intended* consequences (e.g. with regard to the detection of undeclared controlled items for customs checks), but also different *unintended* consequences (e.g. with regard to the privacy impact). As has been shown for risk based passenger screening in aviation security, this may entail a range of possible trade-offs, not only between intended and unintended consequences, but also within these two categories (Weydner-Volkmann 2017): It was shown that introducing certain variants of the risk based paradigm to aviation security can reduce some of the existing ethical issues (e.g. the overall privacy impact), but, at the same time, it is also likely to exacerbate other ethical issues (such as the potential for discrimination). Furthermore, it could be shown that such trade-offs differ considerably depending on which variants of the risk based paradigm are meant to be implemented. For border checks, we expect to face similar trade-off effects.

This means that the introduction of risk based approaches for border checks is likely to have both, positive and negative influences with regard to ELSA related forms of impact when compared to non-risk based approaches. In order to be able to analyse such trade-offs and in order to properly demonstrate the outcome of introducing risk based approaches to border checks with regard to ELSAs, we thus have to analyse the *changes in the corresponding types of impact* vis-à-vis non-risk based border checks, as well as vis-à-vis other variants of risk based

border checks, but not so much the impact of certain variants of risk-based screening isolated and by themselves. The latter would amount to a comparison of the impact of risk based border checks with *absence* of border checks. While the complete absence of border checks would ultimately avoid all forms of ELSA related unintended impact, it is currently not a realistic option and hence cannot be considered the proper point of reference for analysing the changes with regard to ELSA related impact.

Nevertheless, due to the focus of TRESSPASS, much attention should be given in the definition of the relevant types of ELSAs so as to adequately reflect the project's focus on risk based forms of border checks. Ultimately, such 'adequate reflection' must depend at least in part on the outcome of WP1's definition of a risk based border management concept (deliverable D1.2) and the outcome of WP2. Hence, the typology of ELSAs developed in this report may need to be adapted later-on in the project as part of the TRESSPASS framework for assessing the direct ethical, legal and societal impact of risk based screening concepts (deliverables D9.7 and D9.8). It will also need to be adapted to how ethics will be integrated in WP6's overall approach to designing and assessing the CONOPS for border checks.

2.5 Defining the types of relevant ELSA related issues as part of a typology

The present report is intended to identify potential ELSA related *issues* of risk based border checks. Hence, our typology will focus on *unintended consequences* of border checks, rather than also including a discussion of the ethical, juridical and societal merit of the intended consequences, i.e. of the various purposes of border checks. The reason for this is, on the one hand, that the typology is meant as a basis for an ELSA evaluation framework that helps regulators and decision makers to better understand the 'ethical costs' of introducing different forms of risk based border checks. As such, the framework will also form input to other work packages, so as to develop strategies to minimize or mitigate such costs, especially with regard to the usage of enabling technology.[5] On the other hand, this ethical evaluation framework will complement other evaluation tools to be developed as part of TRESSPASS, which will reflect how well risk based border management attains the purposes of border checks (among others by means of red teaming exercises in Task T4.4) as well as how throughput of travelers is impacted by it.

For the intended ethical evaluation framework, this entails that we *will not aim at deciding whether or not certain gains* with regard to the intended purposes of border checks *are worth the costs* with regard to ELSAs. We believe that in democratic societies, such decisions ultimately have to remain part of the political process. Instead of some form of ethical 'green- or red-lighting' of how European societies should or shouldn't choose to organize border checks, we aim at providing regulators, decision makers and the interested public *the intellectual tools to understand the normative impact on the travelling public* that is to be expected when implementing risk based border checks; we aim not at *deciding on the ethical permissibility* of practices at BCPs, but at *making the implied valuations explicit* that are entailed in certain forms of risk based border checks. In doing so, the ethical typology and the subsequently developed ethical evaluation framework is meant to inform decision making, including political processes of deliberation.

[5] For an overview over how different aspects of ethics are addressed in different tasks and work packages within TRESSPASS, please refer to Annex G in deliverable D9.3. This deliverable is also a good starting point to understand how research ethical requirements will be met throughout the duration of the project.

A typology, in this sense, is not meant to cover uniquely occurring situations of conflicting values, i.e. conflicts that are exceedingly rare or cannot be foreseen at all. According to Bernhard Waldenfels (2013, 65–68), the differentiation of the typical from the a-typical is a fundamental ordering principle that rests upon the possibility of *contextual repetition*: Even though no two occurrences of a type are really identical, we still perceive them as of the same kind – we gloss over the ever remaining dissimilarities *as we perceive the two differing occurrences as repetitions of the same*. What gives reason to our experience of something in such a repetitive fashion is its relation to our actions in a situational context: Differing occurrences appear as a repetition of the same because they affect us similarly and/or we can successfully deal with them in the same way as part of our courses of action. In this pragmatic stance of conceptualization, we follow a hermeneutical reading of John Dewey that has been outlined earlier (Weydner-Volkmann 2018, 50–101).

In this sense, a typology of ELSA related issues of border management will identify, in a structured fashion, *recurrent normative conflicts that relate in similar ways to experiencing the impact of the two main functions of border checks on the travelling public and that can be dealt with in similar ways*. This way, the typology is developed from the start as an intellectual tool for decision making with regard to the organization of border checks.

3 TYPOLOGY OF ELSAS FOR RISK-BASED BORDER CHECKS

3.1 Structure of the typology: Three categories of ELSA related types of issues

With regard to a first structure, we can depart from an earlier typology of ethical issues that was developed with regard to passenger screening in aviation security (Weydner-Volkmann 2018; Volkmann 2013a; cf. also Guelke 2011, 35–39). Based on this, we propose three main categories: (A) types of ELSA related issues that directly affect individuals as such; (B) types of issues that affect individuals directly, but as a member of a salient societal group; and (C) types of issues that affect individuals indirectly by impacting a society's basic liberties.[6]

As part of ELSA category A, we have already pointed towards privacy and data protection related issues in section 2.1 above, i.e. situations where the revelatory function of border checks recurrently conflicts with the protection of individual travellers' privacy or of personal data related to them. In contrast, if we focus not so much on the privacy impact on individuals as such, but on the privacy impact on them as members of, say, a religious minority in comparison to the average traveller, potential issues would fall under ELSA category B. Finally, if we look at whether or not travellers in general have effective ways of redress, e.g. in cases of disproportionate privacy infringements, potential issues would fall under ELSA category C.

All three categories deal with the ELSA related impact due to the interplay of the two main functions of border checks. A traveler being allowed or denied to cross the border (access and egress control) is subject to inspection by the border guard as part of the border checks procedures. This may involve physical inspections, e.g. of bags or papers, or the processing of data related to the traveler, e.g. checking a data base for potential warrants. As mentioned in section 2.3 above, this direct negative impact of the revelatory function on the individual is very closely related to privacy and data protection issues. Depending on which specific procedures are used and how far-reaching they are applied for checking a specific traveler, the privacy and data protection impact may differ considerably.

With regard to the access and egress control function alone, the non-intended negative impact[7] is mainly manifest when access or egress is denied. The checking process itself ends here; depending on the reasons for denial, the traveler may need to be transported back to the place of departure, handed over to other law enforcement for investigation and prosecution, have an application for asylum processed, etc. In cases where a false positive during the checking procedure results in denial of access or egress, this may be seen as the extreme negative case of impact on the individual, especially as they are likely to experience

[6] As part of XP-DITE's ethical framework, a fourth category included the dimension of acceptance amongst the flying public (Volkmann 2013a). In TRESSPASS, this dimension will be taken into account separately as part of Task T6.3. For this, TRESSPASS will cooperate with the H2020 project PERSONA (Privacy, ethical, regulatory and social no-gate crossing point solutions acceptance) so as to integrate acceptability data as part of design criteria for border check procedures.

[7] As outlined above, this does not cover aspects of *how well* the intended purpose is fulfilled, i.e. if potential threats go unnoticed. Such questions will be dealt with as part of other work packages in TRESSPASS, e.g. in Task T4.4.

further impact, like being subject to law enforcement processes, or the inability to conduct business, meet with friends and family, spend a vacation, etc.[8]

To understand how this typology deals with such cases of false positives, three forms need to be distinguished: (1) truly unique cases of false positives; (2) recurrent false positives for individual persons, independent of salient social groups; and (3) recurrent false positives for individuals as members of a salient social group. As mentioned in section 2.5 above, the first form of false positives does not cover *typical* cases of ELSA related impact, because they cannot be seen as repetitions of the same with regard to the logic of border checks due to their unique status. At the same time, however, it must be recognized that *the general form* of false positives made up of those unique cases *will repeatedly occur* every now and then in the border checking procedures (inadvertently, but also willingly provoked, e.g. by border guards abusing their power). In order to address this fact, the typology will check for possibilities of legal redress and for the provision of accountability during border checks. Such unique cases of false positives will, therefore, be addressed as part of the ELSA category C, which covers the impact on basic liberties; consequently, as part of the evaluation framework, we will then analyze how the introduction of risk based strategies of border management is likely to impact the possibilities of legal redress and accountability for such cases of false positives.

On the other hand, the third form of false positives (recurrent for individuals as members of a salient social group), falls neatly into ELSA category B, which covers types of recurrent impact on individuals as members of a social group that is considered salient. Salient, here, refers to societal groups that are vulnerable to negative impact due to structural or historical disadvantages – like religious minorities, women, disabled persons, etc.[9] Many of those salient groups are explicitly recognized as protected in the legal non-discrimination frameworks as well as in the relevant regulation (cf. EU 2000 Art. 21, 2016a Art. 7).

The remaining, second form of false positives (recurrent for individuals, but not as members of such a salient social group), is a more problematic case, especially when seen in regard of risk based border management. For non-risk based border checks, such forms of false positives may occur when deliberately provoked for *that specific person* or when persons have certain *personal features* (e.g. they look very similar to a known and wanted person). While such cases are probably reasonably rare and may be addressed similarly as unique forms of false positives – i.e. as part of seeking legal redress (e.g. on the basis of EU 2000 Art. 20) – for

[8] As part of this typology, we will only consider "false positives" with regard to the purposes of the law (e.g. the prevention of terrorist attacks). For a comprehensive ethical assessment, this leaves an "edge case" where a denial may be a true positive with regard to the legal grounds (e.g. a traveler is correctly denied entry, but may still be seen as ethically controversial (i.e. other ethical reasons may justify entry). We consider such questions out of scope for this report, as it does not deal with border checks per se, but rather with the related legislature and policy processes. Deliverable D9.9 will report on a wider ethical context as part of guidelines for decision makers.

[9] For the concept of salient social groups, cf. Altman (2015). The concept of a salient social group is helpful to differentiate legitimate forms of differential treatment from illegitimate, discriminatory forms: Since, for any form of differential treatment, we can artificially construct a social group that is put at an (dis-)advantage, it makes sense to limit the normative label of discriminatory effects to cases where *specific groups that are commonly considered to be vulnerable or put at a structural societal disadvantage are negatively affected.* Hence, it can be considered legitimate to offer discounts to children for admission prices (and, effectively, demand higher prices for adults), but discriminatory to demand higher prices for disabled persons or religious minorities.

risk based border checks, the case may be very different: If, for example, some form of pattern recognition is applied to all travelers in order to identify persons that should be further examined, some of the positive matches will be *false* positives. It is quite possible, then, that these individuals will fit the pattern recurrently – and hence be repeatedly examined further and possibly be repeatedly denied border crossings.

Here, the group of persons affected may not be members of a salient social group, but neither do we "artificially" construct this group as part of the ethical evaluation. Rather, this group is created due to the pattern recognition criteria. As part of the typology to be developed here, such cases will be covered in ELSA category B, since they affect persons in similar ways to discriminatory effects (qua being counted as members of a certain group of persons) and because we can address such issues similarly (by addressing the way categorization works as part of the pattern recognition process). We are, then, broadening category B from being restricted to typical discrimination issues (regarding disproportionate impact on salient social groups), to a more general understanding of unfair distribution of the impact across social groups.

Following this broader understanding, we can then also include another group of persons that may be affected adversely (and potentially disproportionately), but that is unlikely to constitute a salient social group in the sense outlined above: Depending on the kind of data collected and processed as part of the risk analysis, it is possible that border checks may imply privacy intrusions and personal data issues for people who are not crossing the border at all (e.g. when checking the claims of persons regarding the reasons for their stay against information gathered from data mining in social media).

While ELSA category A can, therefore, remain restricted to "privacy and data protection" issues, ELSA category B will be broadened to cover "unfair distribution of impact across different social groups". ELSA category C, finally, will cover "restrictions of societal freedoms and liberties".

Consistent with TRESSPASS's role as an innovation action (applying earlier, more fundamental research activities), the following definitions of the risk types are based on the ones defined as part of XP-DITE's framework for ethical evaluation (Volkmann 2017; cf. also Guelke 2011), but they are adapted in the light of further research on risk-based screening (Weydner-Volkmann 2017) as well as in connection to data protection issues and the different situational context of border checks.

3.2 ELSA category A: Privacy and data protection

The concept of privacy is notoriously hard to define and has rightly been labeled "a concept in disarray. Nobody can articulate what it means" (Solove 2009, 1). We follow Daniel Solove (2009, 40) in not attempting to define a singular meaning or an essence of privacy. Rather, in continuation of our (and also his [10]) methodological approach of a Dewey-inspired pragmatism, we will identify and differentiate types of "privacy aspects" in relation to the revelatory function of border checks. These types of aspects may, then, be considered to belong to a cluster of issues united by what Ludwig Wittgenstein called "family resemblance",

[10] While Solove (2006) develops a "taxonomy of privacy", his aim is to identify surveillance and interrogation issues as actions that cause privacy problems in the legal context. His pragmatic goal, hence, is very different from our own and his taxonomy, although helpful, will not suffice as a means to identify relevant privacy and data protection aspects of border checks.

rather than one clear-cut definition.[11] Understood in such a way, one prominent trait of "privacy aspects" refers to spatial areas, parts of the human body and certain types of information that commonly enjoy protection and shielding from others, so as to allow for respect and free development of an individual's personality. In the following sub-chapters, the concept "privacy" will be differentiated and, through this, its meaning clarified.

With regard to the concept of data protection, matters are not much easier. As Ralf Poscher (2017, 131) writes on the status of data protection as a fundamental right in Europe:

> *A closer look … reveals that Europe is still not at ease with the right to data protection. Above all, it is not clear what the right to data protection is actually about. What, as a substantive matter, does the right actually protect? Fundamental rights usually protect a general or specific liberty or equality interest. But what, specifically, should that be in the case of the right to data protection. This is a question that has haunted the right to data protection since its origins and has been at the center of a more recent wave of criticism leveled against the right, especially in Germany.*

At the core, he argues that data protection is not a fundamental right on its own, protecting specific liberties and equality interests, but rather, in a subsidiary sense, "a systematic enhancement of other fundamental rights", such as "the right to personal freedom in the German constitution, the right to privacy in the Charter of Fundamental Rights of the European Union, or the right to respect for the privacy of the home and family life in the European Convention on Human Rights" (Poscher 2017, 136). He continues that data protection rights are essentially about *abstract dangers*:

> *The collection of data as such does no harm. This has often been expressed with the idea that data has to become information in certain contexts before it can prove its relevance. It is only the use of data in certain contexts that might cause a violation of liberty or equality interests. The collection of personal data about political or religious convictions … is generally prohibited, for example, because of the potential that it could be misused by the state to discriminate against certain political or religious groups … It does not require concrete evidence that misuse of the data has taken place, or even that such a misuse is about to occur. (Poscher 2017, 137)*

Consequently, he argues that, when dealing with issues of data protection, it must be spelled out to what extent a certain form of data collection poses such an abstract danger for the exercise of what kind of fundamental right (Poscher 2017, 137). We will follow this idea as part of our pragmatic typology. Consistent with our overall structure, direct forms of impact on individuals will be discussed in this category, while more general protections against the misuse of data will also form part of ELSA category C.

3.2.1 Intrusion into spatial privacy

This type of impact relates to places where travelers can put any items they choose or need to bring along with them, but do not want to carry in plain view. The most prominent examples of the spatial aspect of privacy in the academic discussion are places that offer seclusion like someone's home (DeCew 2015). However, due to the nature of border checks, such places

[11] Cf. Solove (2009, 40–42): "For example, in a family, each child may have certain features similar to each parent, and the children may share similar features with each other, but they may not all resemble each other in the same way. Nevertheless, they all bear a resemblance to each other."

are not relevant to our analysis (apart from the special case of travelers in a caravan): A BCP, whether in an airport, seaport or at a land border, must be understood as a transit space, where travelers go in order to get to somewhere else. To insist on a space for personal seclusion while crossing the border, even in a caravan, would be an unreasonable expectation for travelers.

Nevertheless, due to the nature of border checks as a means of access and egress control in traveling, the revelatory function may intrude spatial privacy in a different sense. Typically, the home does not only offer seclusion but also shields personal belongings from the gaze and access of officials and other people. Since persons often travel from one private space (e.g. their home) to another (e.g. a hotel room), they often want to bring personal belongings with them that they do not want others to look at or access.

There can be a wide range of reasons why travelers may want to keep the things they bring along *private*. Some things may reveal information about them (e.g. a particular book they read) or they may want to bring something along that has great non-material value and that they do not want others to access. In many situations, the contents of pockets, bags or suitcases can reveal information about a passenger's health, e.g. if he or she brings along certain medicine or medical devices. In any case, travelers usually have a reasonable expectation that the things they bring along with them can be shielded from the gaze and access of others by putting them in a suitcase, in their pockets or the trunk of their car.[12]

Checking pockets, luggage, or the vehicle – for example in a customs related check – negates that shielding effect, which 'transforms' the insides of pockets, suitcases, purses, etc. into private spaces. At the core of this privacy aspect lies the concept of ownership and our cultural norm that others, including the state, should have only limited disposal over what is ours. The revelatory function of border checks, thus, violates this norm by allowing the border guard to access, gaze at or learn about what is inside.

In times where either much of people's conduct leaves digital traces or where personal interactions and other events in people's lives happen entirely or at least in part digitally, new forms of shielding mechanisms become increasingly important: Privacy settings in apps and social media platforms allow a certain measure of control about how widely certain information about person's conduct is accessible publicly; through encryption-technologies, we can artificially create "shielded virtual spaces", where access to digital information is limited to certain persons and the authenticity of that information can be guaranteed to a high degree – even when the underlying data is publicly accessible. Similarly, some people choose to store certain information only on devices they physically control to further limit the chances of a breach of the shielding effect.

As part of the revelatory function, such "digital shielding" may be removed during border checks. By demanding that a traveler gives up encryption keys, unlocks user accounts or physically hands over electronic devices for further examination of the stored data, border checks may intrude in such *virtual private spaces*, which become increasingly important as the digitalization progresses. Apart from the reasons already outlined above, protecting relevant

[12] There is a rich academic and legal debate about what is to be considered an intrusion into spatial privacy, especially in the context of surveillance. Some scholars (especially in the American legal tradition) have argued that everything visible from a public vantage point can be considered public (cf. DeCew 2015). From this point of view, pockets and suitcases often serve the exact purpose of concealment from public visibility.

research, development or business data when crossing borders has become of notable economic relevance, for individuals just as for businesses and enterprises.

3.2.2 Intrusion into bodily privacy

This type of impact relates to parts of the body or information related to the body (e.g. images, medical information, biometrics, etc.) which passengers do not want officials or security staff to look at, touch, know about or consider in their decisions. While many privacy theorists have "viewed the body as being at the core of privacy" (Solove 2009, 52), Solove argues convincingly that it is less the body itself that is at the center of privacy as it is much more the culturally dependent attitudes towards it,

> "… such as concealment of certain bodily parts, secrecy about specific diseases and physical conditions, norms of touching and interpersonal contact, and individual control and dominion over decisions regarding one's body … Norms of interpersonal contact and nudity gradually shifted toward today's norms of greater concealment and distancing from others. Christian beliefs about the body contrasted sharply with those of the ancient Greeks and Romans." (Solove 2009, 53)

Norms of modesty and "self-ownership of the body" can, thus, vary greatly depending on a person's socialization and cultural background. Despite this contingency of norms across cultures and history, European societies (including most migrants and, in fact, many other societies) have in common that they consider certain minimal standards of modesty appropriate when someone's body or body related information is concerned.

For the purposes of this typology, we may assume that while it will be contingent across cultures *which* parts of the body should be concealed *in which contexts*, the act of "removing" clothes that cover certain body parts[13] always has the potential to intrude into a passenger's sense of privacy. The act of "removal" of clothes that cover the body is of course not limited to physical removal or to physical access below the clothes. Similarly to pockets, we may conceive of clothes as having a shielding effect that protects certain parts of the body from the gaze, knowledge and access of others. Thus, technologies such as the body scanners that create an image of the body will remove this shielding effect because they reveal a certain level of detail about what is below the clothes. Furthermore, clothes also have a certain shielding effect against touching someone's body: physical access to body parts below clothing is widely considered highly sensitive and private.

While clothes do have a certain shielding effect, touching someone's body above the clothes is widely considered to be a sensitive matter, too. Although many people may accept being touched above the clothes in certain well defined circumstances (e.g. a pat down), physical access to the body above clothes is still generally prone to intrude into culturally shared spheres of privacy (Solove 2009, 53).

Apart from gazing at or accessing the physical body in itself, bodily privacy also relates to information about "[…] certain bodily functions, such as urination, defecation, and copulation"[14] (Solove 2009, 54) as well as about health conditions or whether the physical body corresponds to certain standards of beauty and normalcy (Traut et al. 2010, 19). This widens the scope of the concept of "bodily privacy" to encompass also *information related to the body* – which also includes biometric information. While attitudes towards the privacy of

[13] Not all clothes cover the body in this sense: The removal of jackets, for example, is usually unproblematic, since a traveller can be expected to wear another layer of clothes that protect relevant body parts from the gaze of others.

[14] The aspect of copulation also covers (culturally contingent) attitudes towards what body parts are understood in close relation to sexual activity and the privacy of it. Cf. also (Solove 2009, 54–58).

biometric information vary greatly across different societies and individuals, one risk of applying biometric technologies relates directly to bodily information: While facial patterns, fingerprints, gait, etc. are usually not deliberately covered or shielded from public gaze or access, *cataloguing* such information for automatic data processing can remove the shielding effect of being just *some body* among other bodies in a public area, i.e. the registration and cataloguing of biometrical information for automatic processing can remove the shielding effect of anonymity in public places (Petermann and Sauter 2002, 89–93). With regard to border checks, such de-anonymization may not seem of high importance when comparing risk-based border checks to rule based border checks – after all, the checking of visas, Union citizenship, etc. requires identification via passports or other documents anyway. Nevertheless, the collection, processing and storing of (especially hard) biometric identification poses data protection issues, whenever it cannot be reliably excluded that such information may also be used to track travelers beyond the border checking process at the BCP (or re-identify them in the future) and, thus, has the potential to automatically and seamlessly de-anonymize the travelers in other contexts as well.

In this sense, allowing the screeners to access or gaze at parts of travelers' bodies that are normally concealed or not accessible to them, or allowing them to reveal or catalogue information about their body risks intruding into the passengers' bodily privacy. At the core of this issue lie cultural concepts of modesty and our cultural norm of self-ownership of the body, which includes the right to determine the aspects of our own bodies that we wish to keep covered. The revelatory function of border checks, thus, has the potential to violate this norm by allowing the border guards to touch, look at or store information about the travelers' bodies and reveal more than is plainly visible.

3.2.3 Intrusion into private life

This risk relates to information about passengers' personal life (including their emotions and intentions) which they do not want officials or security staff to know about or consider in their decisions and which is not plain to see. While the intrusion into spatial privacy relates to physical and digital spaces and the intrusion into bodily privacy relates to a passenger's physical body, an intrusion into private life relates to information about his or her *distinct personality or character*. More specifically, it relates to details about a person's "familial, political, professional, religious, and sexual associations" (US Supreme Court 2012, Justice Sotomayor, concurring 3), [15] his or her communications (Solove 2009, 61–65), or sexual activity (ECHR 2003; Solove 2009, 54–56) for which there is a reasonable expectancy that they are not publicly known.

Of course, there will be a certain grey area where it is hard to distinguish an intrusion into private life from forms of impact that result from revealing information related to the body – for example in case of information about someone's sexuality. In order to further sharpen the distinction between the two impact types, we propose to interpret forms of impact that are directly related to the traveler as an *agent* or to his or her *personal choices* as intrusive into his or her private life (e.g. the choice about his or her sexual associations or activity). On the contrary, revealing information related to the body about the *results* of personal choice (e.g.

[15] Although originally, this concurring opinion of U.S. Supreme Court Justice Sotomayor relates to GPS surveillance in a very different legal context, the argument presented in this concurring opinion about privacy aspects at stake is very relevant for border checks and other forms of screening in the EU, especially in the context of traveling.

a genital piercing) or that never belonged to the realm of choice at all (e.g. a sexually transmittable disease) will be treated as an intrusion into bodily privacy.

Similarly, when we talk about digital information about a person's life, there is another gray area when trying to distinguish intrusions into private life from intrusions into virtual private spaces when collecting online data, e.g. with regard to social media platforms or cloud computing. As mentioned above, we will consider the collection of information to be intrusion into private spaces whenever there is a reasonable expectancy that this information cannot be accessed by just about any person from the public. This includes chats or forums from closed groups, social media postings with private or friends-only settings and comparable situations.

For forms of intrusion into private life, this leaves the collection and processing of information that has (more or less) deliberately been made public by a person about himself. While accessing such information by itself cannot be seen as an intrusion into privacy (after all, the information has been made public), the systematic collection and compilation of publicly available online information about a person so as to *create profiles on their character or dispositions* goes further than this, as it allows the creation of further (probabilistic) information. This is especially true when the compiled information comes from different online sources and/or when it is posted under different pseudonyms.

Again, the cultural norms of privacy vary greatly in scope and in what should be considered a reasonable expectation of privacy across different societies and throughout history. In relation to sexual privacy, for example, Solove argues:

> "In medieval England, sexual transgression was seen as the community's business. People would frequently launch public accusations about others engaging in forbidden sex. When individuals were caught in sexual iniquity, the church courts demanded a public confession." (Solove 2009, 55)

However, we can observe a strong tendency in European societies to consider social relationships, communications and sexual activity as belonging to a sphere of *personal* or *individual* liberties in the sense that the state has no right to intrude into this realm and limit personal choices or the room for personal development (Parent 1983).

Apart from *information* about a traveler's private life, this type of impact also relates to limiting a traveler's ways of self-expression. For example, by prohibiting jokes or criticism, or by making it mandatory to divest or give up cultural or religious items and garments for further inspection, travelers may be limited in their way of expressing their distinct personality. An even more relevant example is the surveillance of people's behavior, so far as it is known to heighten their self-awareness and cautiousness (Cohen 2000, 1425–26). Especially outside of (usually relatively brief) situations where travelers know they are being interviewed and watched closely (e.g. during interview situations by the border guards), i.e. during the regular travel flow, this can be seen as an implicit restriction of their ways of self-expression as it is likely to cause travelers to monitor their own behavior in order to not stand out too much, to comply with the expected appearance and behavior, to avoid raising suspicion or attracting attention. This *loss of carefreeness* can, thus, also be seen as an intrusion into their private lives.

The word "intrusion" needs further clarification in this case as it does *not* mean that the state shouldn't be involved at all in this sphere. In many cases, we wish for state involvement, e.g. through legislation that *protects* our privacy with regard to other persons. Rather, with regard to BCPs, an "intrusion into private life" relates to the revelatory function of border checks which risks making undocumented and non-obvious sensitive information about a passenger's private life known to the border guards (Parent 1983), or which makes use of processes that limit passengers in their ways of expressing their personality. At the core of this risk lies our

cultural norm that people should have the liberty to determine their own lives within the limits of their rights. If passengers have to fear that during border crossings, the border guards may learn sensitive information about their associations, communications or sexual activity then this can infringe upon their liberty in and outside of the checking situation, just as limiting their ways of personal or religious self-expression can do.

3.2.4 Disclosure of information

While the three previous types of impact relate to intrusions into different sub-aspects of privacy by the border guards during the checking procedures, this type of impact relates to the *disclosure* of information that infringes on the traveler's spatial or bodily privacy (including biometrical information), or of information about his or her private life to other persons than the relevant border guards involved. Even when a certain privacy intrusion may be justifiable as part of the border checking procedures, opening a traveler's suitcase in front of other travelers, or communicating biometric information to other governmental agencies or private actors, for example, should be considered a separate form of intrusion.

In this sense, such sensitive information becoming public or known to people not directly involved in or necessary for the border checking process must at least be considered as a form of indiscreetness. Since – as has been shown before – revealing such information could violate certain cultural norms and undermine travelers in their efforts to maintain different aspects of their "public appearance", many countries have developed laws that protect personal information. Moreover, throughout Europe, legal norms have been developed that make it obligatory to handle sensitive information confidentially and make sure that collected information can only be processed for certain specified purposes and not communicated third parties.

3.3 ELSA category B: Unfair distribution of impact across social groups

While category A "privacy and data protection" refers to the different types of impact that screening measures may have on the individual traveler, the category B "unfair distribution of impact across different social groups" refers to the question of whether certain groups of travelers are disproportionately disadvantaged in relation to others (especially with regard to the privacy and data protection impacts). In other words, it refers to types of unfair distribution between different societal groups, such as discrimination issues.

In the academic discussion around discrimination, it has been noted that not just any conceivable group is relevant in this context, but only "salient" social groups, i.e. groups that are socially relevant in the given context (Altman 2015). Amongst the salient social groups, some can be identified for historic or cultural reasons as vulnerable or disadvantaged and, hence, have been explicitly identified in legal texts so as to protect them against further discrimination (Altman 2015). While this is not an exhaustive list, groups identifiable by sex, gender, race, color, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, minority status, property, birth, disability, age or sexual orientation have been recognized explicitly by the EU to enjoy this protection (EU 2000) and need to be carefully considered.

It is important to realize that the concept of discrimination inherently entails a comparative element (Altman 2015). Depending on the vulnerable social group in question, the relevant reference group may differ from group to group. At the same time, it is not arbitrary in nature. For the different groups, it will, thus, be necessary to identify the relevant reference group.

E.g. for disabled passengers, the relevant reference group would be the majority of non-disabled passengers, while for economically disadvantaged passengers, the relevant reference group would be the assumable minority of financially strong passengers (Altman 2015).

As already detailed in section 3.1 above, we will use a broader understanding for this ELSA category that is not limited to discrimination issues as such. Instead, in order to better capture potential side effects of a risk-based approach to border checks, we will include the impact on societal groups that are newly constructed due to the risk assessment categorization, as well as impact on non-travelers.

3.3.1 Disproportionate impact due to infeasibility of standard checks

This type of impact relates to situations in which it is not feasible for some travelers to be checked in the foreseen standard procedure. Examples could be travelers who are unable to use biometric enrolment or verification procedures or who cannot comply with certain screening procedures due to technical reasons (e.g. when the use wheelchair prevents the use of a body scanner in customs checking procedures). Usually, alternative checking procedures will be used in such situations. Depending on how intrusive the alternative checks are in comparison to the standard checking method, there may be a risk of an intensified privacy or data protection impact for those travelers, for whom standard screening is not feasible. The relevant reference group, then, is the group of travelers subject to the standard screening procedures.

In other cases, the checking procedure may involve cooperation of the individual, e.g. during the verification process of a traveler's identity. For example, the checks may require travelers to reveal their faces to the border guards and, in doing so, remove covering clothes that are religiously or otherwise of great relevance for a passengers personal or religious identity. Requiring them to remove such items may, thus, inhibit or hinder them in living their personal choices or convictions publicly. In the context of aviation security screening, touching religiously relevant headwear has caused irritations in the past (Neiyyar 2011) and, although less prominent here, similar conflicts are to be expected in the context of border checks if similar processes are applied (e.g. in customs checks). Hence, for some vulnerable groups in society, standard checking procedures may be more intrusive compared to a potential majority of passengers for whom the same form of compliance is culturally insignificant. In this case, less intrusive alternative checking methods can mitigate potential disproportionate impacts.

At the core of this type of impact lies the democratic cultural norm of fair distribution of costs. In this sense, privacy and data protection impact (considered as costs of border checks) should be distributed fairly and not affect some societal groups disproportionately.

3.3.2 Disproportionate impact due to accumulation of false alarms

This type of impact relates to situations in which a "false alarm" is triggered at the BCP during the checking process, hence requiring further checks (e.g. as part of second line checks), which in turn may imply additional impact. The definition of what exactly a "false alarm" is can be tricky and depends on the context: *All forms* of checking processes that raise alarms have a certain probability in which an alarm is raised although the traveler should, in fact, be cleared. This could happen because a border guard or biometric system falsely believes that a travel document does not belong to the person holding it (e.g. because the image doesn't seem to match the face or because the facial biometric verification fails). Hence, further checks may be necessary that create additional impact. For risk based border checks, another example

could be named for certain forms of automated anomaly detection systems: Here, whenever an alarm is raised, with a certain degree of probability it will be a false alarm, e.g. due to biased training data for the anomaly detection algorithms. In such a case, a retraining of the algorithms with better-suited data (e.g. from that specific checkpoint) would cause the same behaviors to be considered "normal".

In addition to this form of false alarms, it is also possible that a traveler's behavior correctly raises an anomaly alarm, but that it turns out in subsequent checking that the travelers do in fact not pose a threat. This could be called a "natural alarm", indicating the fact that the pattern recognition is working as intended, but that the alarm can be resolved subsequently.

For false and natural alarms, usually some form of resolution process will follow. Depending on the nature of these additional processes, border checks may thus trigger more intrusive measures. These additional checks (or false denials of entry or egress) may affect some groups disproportionately, if they are more likely to trigger false or natural alarms. For example, in case of the use of automated anomaly detection techniques, travelers that differ from what is expected to be normal (e.g. due to disabilities) can cause natural alarms repeatedly. For such travelers, the probability to be affected by more intrusive second line checks or other alarm resolution processes may be disproportionately higher than for other passengers.

In a similar sense as we have argued in section 3.3.1 above, the democratic cultural norm of fair distribution of costs lies at the core of this type of impact. It indicates that border checks should not disproportionately often cause natural or false alarms and, thus, accumulate further privacy intrusions for certain societal groups.

3.3.3 Disproportionate impact due to false or incomplete external data

This type of impact relates to the proneness of border checks to use false or incomplete data that was not generated at the BCP. It differs from the impact type "false alarms" by relating to the usage of external data input, e.g. from making use of external data bases.

As opposed to aviation security, border checks have made extensive use of external data for quite some time, e.g. by checking passports presented by travelers against external data bases of lost and stolen travel documents. As part of a risk based traveler differentiation approach, BCPs may also make use of external traveler risk profiles (e.g. in form of lists of persons subject to additional checks) or border guards may make use of external information to perform profiling at the BCP (e.g. as part of second line checks to verify claims made by the traveler).

Depending on whether external data is used during border checks, an intensified impact might be caused for vulnerable groups of passengers. From this perspective, it is irrelevant whether the data input is false, i.e. not true to the fact, or whether the data is correct but incomplete, i.e. additional information would have changed the risk assessment (e.g. a risk profile may be correct on the basis of the available information, but additional facts would show that the traveler should not be considered higher risk). Thus, similarly to the impact type of false alarms, it is mainly relevant for how many travelers the external data input falsely causes an intensified impact and whether vulnerable societal groups are disproportionately affected. In addition to discriminatory questions, this type of impact will also cover situations where a (non-vulnerable group of) travelers may be recurrently be falsely considered as high risk due to profiling or pattern recognition techniques.

At the core of this type of impact lies the cultural concept of fair and impartial administration, i.e. the norm that traveler differentiation processes should not lead to disproportionate impact on some groups and that public administration should act on reliable and accurate information.

3.3.4 Impact on non-travelers

While the three previous impact types related to forms of traveler differentiation and unfair distribution of impact across vulnerable social groups, this type of impact relates to whether it is possible that people who don't plan to cross the border might be affected by the border checking process. This may or may not be a discrimination problem, since the group of affected non-travelers could be a kind of cross section across all societal groups. Even so, however, it would still refer to a specific form of disproportionate impact, as the impact of border checks on non-passengers can then hardly be justified by a gain in security.

Thus, this type of impact is mostly relevant for situations in which some checking procedures happen *outside or before* the BCP, e.g. in a land border scenario through sensors that collect license plate data on streets leading towards the BCP. Similarly, collecting information on travelers from public sources, especially from social media, may also affect other persons than the travelers themselves. In such a case, upstream data collection may cause unnecessary privacy intrusions for persons who live or work close to the border or who are merely in some form of contact with persons crossing the border. This is especially problematic if such measures are not overt and can, hence, hardly be avoided by non-travelers.

At the core of this type of impact lies the cultural norm that privacy and data protection intrusions should be justified, i.e. that there should not be unnecessary impact on non-involved third parties, who do not intend to cross the border.

3.4 ELSA category C: Restrictions of societal freedoms and liberties

This category analyses what could be called legal and societal acceptability. In contrast to societal acceptance, the societal acceptability does not so much involve travelers' *opinions* about border checking procedures, but rather an assessment of border checks in the light of core societal values (mainly from a liberal tradition), which describe different aspects of an open society by limiting the power of the state to restrict people in their liberties.

As an indication of what can be considered an "open society" in a European context, we base this category on texts like the Charter of Fundamental Rights of the European Union (EU 2000). While other legal documents such as the European Convention of Human Rights, case law from the European Court on Human Rights or case law from constitutional courts of member states are interesting sources, too, the Charter of Fundamental Rights promises to be a particularly suitable document, because it explicitly refers to the former documents as sources for its own conception and interpretation. [16]

3.4.1 Accosting travelers

This type of impact relates to the idea that an open society should respect the freedom of movement for persons. While, in fact, different laws may be applicable in different contexts, the idea that governmental actions should not subject individuals to unjustified searches or impede their movements is a central liberal conception with a longstanding tradition that reaches back in the form of codified rights to the (British) Magna Charta from 1215 and the Petition of Right from 1628. Within the EU, for example, Union citizens are guaranteed "the right to move and reside freely within the territory of the Member States" (EU 2000, Art. 45).

[16] Of course, we cannot assume that there is an extensive, detailed and clearly defined set of cultural norms shared across Europe. Nevertheless, we can read such legal documents as a codification of individual rights *based on values that are meant to characterize European societies*. Thus, we can read such documents as indications for core societal values of an open society.

Similarly, national constitutional law or legislation protects the closely related individual right to move freely in public places and the individual right not be subject to unjustified searches: In the German constitutional law, for example, the "körperliche Bewegungsfreiheit" guaranteed by Art. 2 II S. 2 and 104 GG not only protects all individuals from being hindered to move to, stay in or leave public places, but also from actions such as being searched by the police or other similar activities (Schmidt 2007, 144–46). Hence, we argue that the concept of freedom of movement can form one aspect to guide our evaluation of how open or restrictive a society is.

Of course, freedom of movement is not an absolute right that entitles a person to enter any place whatsoever; there must be a factual and legal possibility for the person to move there (for example, it does not entitle a person to enter private homes etc.). Hence, in the context of border and customs checks, the right does not entitle just about any person to enter or leave the EU territory without being checked in any way. While border checks generally interfere with the freedom of movement of travelers, regulation can make entry to EU territory conditional to certain requirements for non-citizens (e.g. applying for a visa that is granted only in certain conditions). Border checks can then be used to enforce this regulation, e.g. by denying entry to third country nationals without such a visa. At the same time, however, where persons actually *have the right to enter or leave EU territory* (e.g. in the case of Union citizens), checks beyond verifying eligibility for access or egress have to be legally justified in different ways or else not take place. This is also reflected in the Schengen Border Code, where it is regulated that border checks for Union citizens (and persons of same status) shall normally consist only of a "minimum check in order to establish their identities" and that such a check shall only consist of a "rapid and straightforward verification" (EU 2016a, Art. 8).

In this report, we will not take the details of the legal applicability of "freedom of movement" into account as such. Instead, we propose to interpret this legal concept as implying a society that is characterized by the fact that, so long as it is legally permissible and factually possible, individuals can freely move to, stay in and leave public places as they wish without being approached, stopped or questioned by the relevant authorities. Thus, we interpret the concept of freedom of movement in a way that extends to situations where governmental actions may systematically create obstacles to travelers' movements, so far as they are eligible for access or egress, especially when subjecting them to being impeded, questioned, searched, etc. without specific and individual cause for suspicion.

In this sense, border and customs checks may undermine this idea of "free movement" when the implementation of security measures involves travelers being accosted by the border guards. Intense security measures, high costs in both, monetary and privacy terms on behalf of the travelers, acute surveillance, and a great loss of time will, thus, undermine the intended seamlessness of travelling and contribute to a transformation process that makes European societies more restrictive.

3.4.2 Lack of accountability

This type of impact relates to the idea that when officials like border guards interfere with someone's actions or infringe someone's privacy they must to do so on a legal basis and in a reasonable manner (impact must be proportionate, necessary and sufficient) or else be held accountable for misconduct. At the core of this idea is the cultural concept that governmental actions that interfere with people's lives are only legitimate on a legal basis and that people must have a way to take legal action. We can find different rights in the Charter of

Fundamental Rights of the European Union that specify this idea:[17] Art. 41, for example, codifies the citizens' right to good administration and states that this right includes "the obligation of the administration to give reasons for its decisions" and that inflicted damages have to be made good; Art. 43 makes it necessary to be able to refer to an ombudsman in cases of maladministration; Art. 47 guarantees effective remedy in case of a violation of rights and freedoms (EU 2000).

In the context of border checks, it should therefore be feasible for passengers to hold border guards, supervisors or officials accountable for misconduct or unreasonable treatment in the screening process without fear of further negative consequences for themselves. This means that, in an open society, it should be easy to understand for travelers what rights they have, what kind of behavior they can expect from customs and border guards, and at what point they have the legitimate right to refuse cooperation and/or seek remedy in case of misconduct or unreasonable treatment.

Especially in case of risk based traveler differentiation processes, the reasons for the relevant classifications should not be withheld (at least not in court) so that passengers have the effective ability take legal action. Failing to do so may undermine the liberal idea of accountability and contribute to a transformation process that makes European societies more restrictive.

3.4.3 Restriction of self-determination and misuse of data

This type of impact is closely connected to data protection aspects and relates to the idea that governments should not keep extensive profiles about their citizens' habits and personal choices. As discussed in section 3.2 above, we conceptualize data protection rights as subsidiary in the sense that they are meant to systematically enhance other fundamental rights. Intrusions that can be attributed directly to specifiable individuals (e.g. as part of the border and customs checking process) are part of ELSA category A. In contrast, this type of impact refers to more abstract forms of intrusions, such as when large amounts of surveillance data is stored for long periods of time, but it is not yet clear who will be affected in what ways by the collection. In these cases, travelers may be substantially hindered in their freedom to make self-determined choices, unless they understand what personal information is known to others, including government officials. In the German context, this lead to the formation of a separate right, the right to informational self-determination. Here, it becomes very clear that this right exists to systematically enhance other fundamental rights.

Apart from a reference to data protection and fair data processing, Art. 8 of the Charter of Fundamental Rights of the European Union also states that personal data shall only be collected and processed "for specified purposes" (EU 2000). In an effort to harmonize data protection regulation across Europe, the General Data Protection Regulation (GDPR) was adopted and came into force on 25 Mai 2018. It is accompanied by the so called Law Enforcement Directive, that specifies data protection principles in the context of law enforcement. Apart from the fact that any form of border and customs checks must be compliant with the (then) current data protection legislation, it helps to take a closer look at the core principles that guide the current data protection regime in order to provide the basis for an assessment of the impact with regard to restrictions of societal freedoms and liberties.

[17] It is important to stress that these codifications are cited solely for the purpose of identifying fundamental societal values from a mainly liberal tradition which are meant to characterize European societies, not for the purpose of a legal analysis.

Largely consistent with previous data protection regimes (Raguse 2008, 11–12), the GDPR explicitly identifies six principles relating to the processing of personal data (EU 2016c, Art. 5):

a) lawfulness, fairness and transparency (covered in sections 3.4.2 and 3.4.4);
b) purpose limitation (collect and process only for the specified purposes);
c) data minimization (collect and process only what is necessary);
d) accuracy (covered in section 3.3.3);
e) storage limitation (keep only as long as necessary);
f) integrity and confidentiality (security of the data).

As a seventh principle, it states that those persons or entities determining the purposes and means of the data collections have to demonstrate that these principles have been met. This means that the data protection regime functions as a general prohibition of data collection and processing unless these principles have been met. In the context of border and customs checks, a range of data collection and processing activities take place, e.g. when processing biometric data to verify the identity of a traveler, and it needs to be made sure that these principles are properly met, e.g. that after verifying the identity, no biometric data is retained.

In this example, since it is notoriously difficult to protect biometric passenger data, it can be seen as a general best practice to avoid long-term storage and to leave the traveler in as much control as possible over their biometric data, e.g. through token based biometric verification via electronic passports (Petermann and Sauter 2002). Border and customs check procedures that accumulate many sensitive data and protect them inadequately risk unauthorized or accidental disclosure of private passenger data, i.e. they expose travelers to misuse of that data by other actors than the original collectors.

Furthermore, the principle of purpose binding is of particular importance. While there need to be legitimate grounds to collect and store personal passenger data in the first place, there is also a great risk that this data may be accessed or processed for different purposes than originally justified and intended (“mission creep”). Storing or processing personal data and failing to implement rigid control mechanisms risk that such data will be misused by the same actors that originally collected the data.

However, even if there would be no collection or storage of personal data at BCPs *per se*, border checks may still restrict travelers’ self-determination or expose them to data misuse. Especially as part of a risk based approach to border management that uses some form of traveler differentiation, border guards may simply make use of previously collected data or simply use the “output” of personal data processing, as it is currently done in aviation security screening at some airports in the world. Here, upstream agencies perform a risk assessment of certain passengers by processing personal data, so the security screening checkpoint needs only to collect data that is needed to establish the passengers’ identities (Weydner-Volkmann 2017).

Nonetheless, by making use of such “external passenger profiles”, border and customs checks create a dependency between the effectiveness of the security provision and the collection and processing of travelers’ personal data: the level of additional security to be provided depends directly on the creation of risk profiles that flag a person, e.g. for second line checks. Hence, border and customs checks may create a demand for more extensive data collection on travelers and further surveillance measures. An example for this would be the retention and processing of PNR data (EU 2016b).[18] In addition to that, such risk profiles may also be

[18] The PNR data collection and retention is currently under legal scrutiny. An opinion of European Court of Justice (ECJ 2017) deemed the envisaged PNR data exchange with Canada incompatible with the EU

created at least in part by intelligence services that are *de facto* much less bound to the scrutiny of data protection oversight. Hence, using externally developed traveler risk profiles or categorizations may very well create a demand for extensive data collection on passengers and the potential misuse of such data.

Hence, both the collection and processing of personal data at the border, as well as the usage of externally produced profiles of categorization may restrict travelers in their right to self-determination. In an open society, it is therefore necessary to mitigate such risks by ensuring that the principles of the data protection regime are followed as much as possible.

3.4.4 Lack of transparency

This type of impact relates to the democratic ideal that governmental actions should be transparent. Article 42 of the Charter of Fundamental Rights of the European Union, for example, states that any citizen or resident in the EU has the right to access documents of the EU institutions (EU 2000). The idea of administrative and political transparency is closely connected to governmental accountability, but it goes beyond the guarantee of legal remedy in case of maladministration by aiming at a strengthening of democratic participation (Wagner 2015, 133).

Of course, in security contexts like border and customs checks, not all procedures can be fully transparent. The revelatory capabilities of verifying the identity of a traveler and the authenticity of travel documents differ from technology to technology and the detection rates of different customs screening equipment will similarly vary to a certain degree. This means that the effectiveness of customs and border checks in general and of the revelatory function in particular can be reduced by well-prepared actors who want to cross the border illegitimately by exploiting known weaknesses. For this reason, detection rates, interview questions, risk indicators, procedural documents, etc. are classified in many cases. Here, full transparency would undermine the intended security gain of some procedures.

However, while it may be justified to withhold certain detailed information that may allow the exploitation of weaknesses, border and customs checks may be seen in the context of a broader current trend in the security sector towards less transparency on behalf of governmental actions and toward greater transparency on behalf of the citizens subject to those actions (Wagner 2015, 134–37).

Thus, in-transparency of border and customs checks should still be considered problematic if it means that interested travelers or the democratic public do not understand what is happening during the checking process and what options and rights they have, what data is collected for what purpose and what information the border guards can, in fact, learn, access or store for how long. All of these aspects promote processes and structures that make governmental security measures opaque and restrictive, and they undermine them in their democratic legitimacy, since passengers may not understand to what end they have to suffer the intrusion into their privacy.

legal framework and also identified some aspects (e.g. the length of storage) that could also be seen to apply to the current EU PNR data retention.

4 INTEGRATION WITH THE OVERALL CONOPS FRAMEWORK

Following our stance of philosophical pragmatism, as mentioned in section 2 above, we do not claim that the typology is an adequate representation of some sort of "reality of ethical and social norms in relation to border checks". Rather, we claim that the typology is a *helpful tool* for the identification of relevant potentially conflicting values, which will allow an ethical evaluation of those changes that result from the implementation of risk based border management, including the design of new BCPs.[19]

To this end, we will develop impact assessment scales for each of the ELSAs identified in the typology. Ultimately, in deliverables D9.7 and 9.8, we aim at presenting a method for evaluating the impact of risk based border management along these scales. This is based on earlier works (Volkmann 2013b, 2017). This will provide (qualitative) performance data with respect to the ELSAs identified here in this report, i.e. ethical Performance Indicators (PIs) that can be used for design and evaluation of specific BCPs.

As mentioned above, the ability to evaluate the ELSA related impact of different forms of border checks will allow informed decision making as part of the design process: It will provide awareness regarding the ethical trade-offs involved and provide the intellectual tools necessary to make conscious design choices about normative concepts like privacy, data protection, non-discrimination, etc. (Ethics and Data Protection by Design, EDPbD). This includes the positive as well as the negative effects of introducing risk-based border checks.

The aim of this chapter is to provide "rump scales" so as to give a first indication of what will be assessed by the evaluation framework and how we plan to integrate this assessment as part of the overall CONOPS framework.

TABLE 4-1 RUMP SCALES FOR ELSA CATEGORY A

	Negative Pole	↔	Positive Pole
Overall impact on privacy and data protection	*Overall intrusion into privacy and private data*	↔	*Overall respect of privacy and private data*
Intrusion into spatial privacy	Intruding into physical and virtual private spaces	↔	Respecting physical and virtual private spaces
Intrusion into bodily privacy	Exposing travelers' bodies	↔	Respecting travelers' bodily public appearance
Intrusion into private life	Undermining personal public appearance	↔	Respecting personal public appearance
Disclosure of information	Indiscreetness	↔	Discreetness

[19] A more extensive discussion on the epistemic basis of this typology can be found in earlier texts (Volkmann 2013a; Weydner-Volkmann 2018).

TABLE 4-2 RUMP SCALES FOR ELSA CATEGORY B

	Negative Pole	↔	Positive Pole
Overall fairness in distribution of impact	*Discriminating against diversions from the norm or recurrent impact of errors*	↔	*Respecting diversions from the norm and low recurrency of errors*
Disproportionate impact due to infeasibility of standard checks	Disproportionate impact in case of infeasibility of standard checks	↔	Equal or less impact in case of infeasibility of standard checks
Disproportionate impact due to accumulation of false alarms	High proneness to cause higher impact in alarm or rejection resolution	↔	Low proneness to cause higher impact in alarm or rejection resolution
Disproportionate impact due to false or incomplete external data	High proneness to cause more intrusion due to false or incomplete external data	↔	Low proneness to cause more intrusion due to false or incomplete external data
Impact on non-travelers	High probability or severity for impact on non-travelers	↔	Low probability or severity for impact on non-passengers

TABLE 4-3 RUMP SCALES FOR ELSA CATEGORY C

	Negative Pole	↔	Positive Pole
Overall contribution to restrictions of societal freedoms and liberties	*Contributes to restricting societal freedoms and liberties*	↔	*Respects openness of society*
Accosting travelers	Intense security experience	↔	Seamless traveling
Lack of accountability	Low accountability in border checks	↔	High accountability of border checks
Restriction of self-determination and misuse of data	Undermining protections and misuse of personal data	↔	Preserving protections of personal data
Lack of transparency	Low transparency of border checks	↔	High transparency of border checks

For optimum utility and impact these instruments need to accompany the CONOPS development work which involves a process of data collection and synthesis on the subject of the activities that people perform when going about the work in relation to border crossing point management or associated activities. The development of CONOPS representations of real-world operations involves the use of number of heuristics outlined in D6.1 “Observational studies methodology and research framework”. While this framework examines a broad range of factors that contribute to operational performance, particularly from a human factors perspective, but also how human activity is mediated by technology as well as formal and informal rules, the ethical questions in this report form an integral part of this approach.

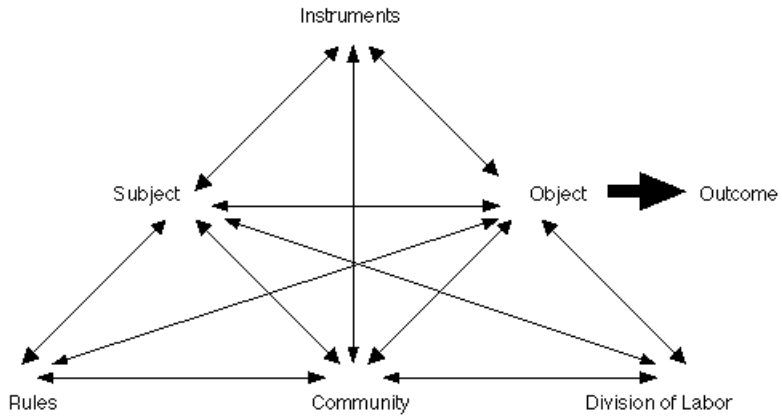

FIGURE 1: ACTIVITY SYSTEM FRAMEWORK

Figure 1 illustrates how an individual's object-orientated activity (i.e. activity towards specific goals), mediated by technology (instruments), towards a motivated socially meaningful outcome, and in an overall division of labor, is also mediated by rules including ethics, regulation, legal frameworks, and cultural norms (Engeström 1987). These are contextual in nature and need to be understood in relation to their operational context, which includes the organizational structure, professional culture, and also geographical, and possibly geopolitical features when it comes to border crossing points.

From this point of view, the methodology and instruments discussed here are part of the methodology that will instruct and construct the CONOPS, addressing the "rules" aspect of the diagram. This will work in two directions. Data collected from activity in WP6 working with end-users with a view to understanding their operational processes, systems, structures and activities will also provide data complementing and further informing this typology. Likewise, activity within WP9 that produces information about relevant ELSAs regarding end-user activity will be fed-back into the CONOPS framework. The CONOPS itself, thus, provides (among others) also information on ELSA related, non-intended impact on travelers and feeds it back to the tool development tasks, pilot planning, and to support evaluation.

5 CONCLUSIONS

In this report, we have identified the ethical, legal and societal aspects that we foresee to become relevant as unintended negative impact for risk based border management concepts. As such, it documents the first step towards the definition of an Ethics and Data Protection by Design (EDPbD) approach for TRESSPASS's single cohesive risk-based border management concept for air, maritime and land border crossing points.

Chapter 2 of this report provides a conceptual description of border checks that allows the systematic identification of relevant ELSAs along three main categories:

RELEVANT ELSAS FOR RBBM

ELSA category A: Privacy and data protection	ELSA category B: unfair distribution of impact across different social groups	ELSA category C: restrictions of societal freedoms and liberties
Intrusion into spatial privacy	Disproportionate impact due to infeasibility of standard checks	Accosting travelers
Intrusion into bodily privacy	Disproportionate impact due to accumulation of false alarms	Lack of accountability
Intrusion into private life	Disproportionate impact due to false or incomplete external data	Restriction of self-determination and misuse of data
Disclosure of information	Impact on non-travelers	Lack of transparency

Chapter 3 of this report then identifies and defines 12 types of potential, ELSA related forms of impact as part of a structured typology, grouped into those three main categories of ELSAs:

Based on this typology, deliverables D9.7 and D9.8 will develop a framework for comparative assessment of risk based screening concepts for border checks. In preparation for this, Chapter 4 has identified a rump scale for each type of impact. Unintended negative impact will be evaluated in a comparative fashion along these scales, thus allowing a better understanding of the positive as well as the negative effects of introducing risk based border checks – which will also allow the development of ways to mitigate or minimize such impact "by design".

REFERENCES

Altman, Andrew. 2015. “Discrimination.” In *The Stanford Encyclopedia of Philosophy*, edited by Edward N. Zalta, Fall 2015. http://plato.stanford.edu/archives/fall2015/entries/discrimination/.

Cohen, Julie E. 2000. “Examined Lives: Informational Privacy and the Subject as Object.” *Stanford Law Review* 52 (5): 1373–1438.

DeCew, Judith. 2015. “Privacy.” In *The Stanford Encyclopedia of Philosophy*, edited by Edward N. Zalta, Spring 2015. http://plato.stanford.edu/archives/spr2015/entries/privacy/.

Dewey, John. 1981. *The Later Works Volume 1: 1925, Experience and Nature*. Edited by Jo Ann Boydston and Sidney Hook. Carbondale (Ill.): Southern Illinois University Press.

ECHR. 2003. “Judgment by the European Court of Human Rights (Fourth Section), Case of Peck v. United Kingdom, Application No. 44647/98 of 28 January 2003.”

ECJ. 2017. Opinion 1/15 of the Court (Grand Chamber) 26 July 2017 CURIA. ECJ.

Engeström, Yrjö. 1987. *Learning by Expanding: An Activity-Theoretical Approach to Developmental Research*. Helsinki: Orienta-Konsultit.

EU. 2000. *Charter of Fundamental Rights of the European Union*. Vol. 2000/C 364/01. http://www.europarl.europa.eu/charter/pdf/text_en.pdf.

———. 2016a. *Regulation (EU) 2016 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the Rules Governing the Movement of Persons across Borders (Schengen Borders Code)*. *CELEX*. Vol. 32016R0399. https://publications.europa.eu/en/publication-detail/-/publication/42fba6c3-f0c5-11e5-8529-01aa75ed71a1.

———. 2016b. *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*. *OJ L 119*. http://data.europa.eu/eli/dir/2016/681/oj.

———. 2016c. *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 L*. Vol. 119. http://data.europa.eu/eli/reg/2016/679/oj/eng.

Grabitz, Eberhard, Meinhard Hilf, and Martin Nettesheim. 2018. *Das Recht der Europäischen Union: Band I: EUV/AEUV, Rechtsstand: Mai 2018*. 64. Aufl. Das Recht der Europäischen Union. München: Beck, C H.

Guelke, John. 2011. “DETECTER: Detection Technologies, Terrorism, Ethics and Human Rights. Quarterly Update on Technology 10 (D12.2.10).” DETECTER (FP7-SEC-2007-217862). http://www.detecter.bham.ac.uk/documents.html.

Neiyyar, Dil. 2011. “Sikhs Upset about Airport Security Checks on Turbans.” BBC News. February 24, 2011. http://www.bbc.co.uk/news/uk-england-12558996.

Parent, W. A. 1983. “Privacy, Morality, and the Law.” *Philosophy & Public Affairs* 12 (4): 269–88.

Petermann, Thomas, and Arnold Sauter. 2002. “Biometrische Identifikationssysteme. Sachstandsbericht, Büro Für Technikfolgenabschätzung Beim Deutschen Bundestag (TAB).”

http://www.itas.kit.edu/pub/v/2002/pesa02a.pdf.

Poscher, Ralf. 2017. “The Right to Data Protection. A No-Right Thesis.” In *Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair*, edited by Russell A. Miller, 129–41. Cambridge University Press.

Raguse, Maren. 2008. “Legal Evaluation Report.” PRISE Deliverable D3.2. PRISE. http://www.prise.oeaw.ac.at/docs/PRISE_D3.2_Legal_Evaluation_Report.pdf.

Rule, James. 1974. *Private Lives and Public Surveillance. Sovial Control in the Computer Age*. New York: Shocken Books.

Schmidt, Rolf. 2007. *Grundrechte: sowie Grundzüge der Verfassungsbeschwerde*. 9. Aufl. Grasberg bei Bremen: Schmidt.

Solove, Daniel J. 2006. “A Taxonomy of Privacy.” *University of Pennsylvania Law Review*, 477–564.

———. 2009. *Understanding Privacy*. Cambridge, Mass.: Harvard Univ. Press.

Traut, Andreas, Michael Nagenborg, Benjamin Rampp, and Regina Ammicht Quinn. 2010. “Körperscanner – Sicherheiten Und Unsicherheiten.” *Forum Kriminalprävention* 1: 14–20.

US Supreme Court. 2012. “United States v. Jones 565 U.S. ___ (2012).” https://supreme.justia.com/cases/federal/us/565/10-1259/.

Volkmann, Sebastian. 2013a. “Ethical and Legal Requirements for System Design.” D7.1. XP-DITE Deliverable. Albert-Ludwigs-Universität Freiburg. https://doi.org/10.6094/UNIFR/13037.

———. 2013b. “Methods for Assessment and Quantification of Compliance with given Ethical Requirements.” D7.3. XP-DITE Deliverable. Albert-Ludwigs-Universität Freiburg. https://doi.org/10.6094/UNIFR/13816.

———. 2017. “Updated Methods for Assessment and Quantification of Compliance with given Ethical Requirements.” D7.10. XP-DITE Deliverable. Albert-Ludwigs-Universität Freiburg. https://doi.org/10.6094/UNIFR/14020.

Wagner, Edgar. 2015. “Die Geschichte der Öffentlichkeit in Theorie und Praxis.” In *Transparenz contra Geheimhaltung in Staat, Verwaltung und Wirtschaft: Beiträge auf der 16. Speyerer Demokratietagung vom 23. bis 24. Oktober 2014 an der Deutschen Universität für Verwaltungswissenschaften Speyer*, edited by Hans Herbert von Arnim, 131–42. Schriftenreihe der Deutschen Universität für Verwaltungswissenschaften Speyer 229. Berlin: Duncker & Humblot.

Waldenfels, Bernhard. 2013. *Ordnung im Zwielicht*. 2., um Ein neues Vorw. erg. Aufl. Übergänge 61. Paderborn: Fink.

Weydner-Volkmann, Sebastian. 2017. “Risk Based Passenger Screening in Aviation Security: Implications and Variants of a New Paradigm.” In *Rethinking Surveillance and Control. Beyond the “Security versus Privacy” Debate*, edited by Elisa Orrù, Maria Grazia Porcedda, and Sebastian Weydner-Volkmann, 49–83. Sicherheit Und Gesellschaft. Freiburger Studien Des Centre for Security and Society 12. Baden-Baden: Nomos.

———. 2018. *Moralische Landkarten der Sicherheit. Ein Framework zur hermeneutisch-ethischen Bewertung von Fluggastkontrollen im Anschluss an John Dewey*. Baden-Baden: Ergon.

Zurawski, Nils. 2015. *Technische Innovationen und deren gesellschaftliche Auswirkungen im Kontext von Überwachung*. Schriftenreihe Sicherheit 16. Berlin: Forschungsforum Öffentliche

Sicherheit.

LIST OF TABLES

LIST OF FIGURES