Summary

1 Introduction

It is of essential importance to correctly determine a person's identity in the context of a criminal case. On the one hand, innocent persons who fall victim to the mixing up of different identities may experience serious consequences for years after. On the other, those who are 'guilty' can avoid problems by using false identities. As of 2010, the *Act on the Identification of Suspects, Convicts and Witnesses* (WIVVG) thoroughly changed the methods of identification of suspects and convicted persons (as well as of witnesses, which fall beyond the scope of the present study) in Dutch criminal law. Aim of the WIVVG is to guarantee correct identification and verification to the extent possible in the entire criminal justice chain. The question remains, however, how to maintain the same accuracy in cases that require exchange of information with other EU Member States on suspects and convicted persons i.e. incoming and outgoing information on those persons' identities. Our study addressed this question. First, we charted vulnerabilities in the exchange processes of identification data between the Netherlands and other EU Member States and second, we focused on the question whether biometric methods can provide solutions to problems with identification as experienced by the competent authorities.

2 Research questions

First question: which vulnerabilities occur in the exchange processes of identification data concerning suspects and convicted persons in the context of EU law enforcement cooperation?

Vulnerabilities can be distinguished as follows:

(a) Vulnerabilities related to the effectiveness of identity determination during the phases of investigation, prosecution, trial and execution of sentences.

First, exchange of incorrect personal data between the Netherlands and other EU Member States may result in failure to apprehend the actual suspect or sentencing the correct convict (vulnerability a1). Vulnerabilities can be distinguished further into: (a1a) administrative and technical mistakes or inaccuracies; (a1b) defective implementation of rules; (a1c) costs and efforts of additional investigations.
Second, there is the risk of identity misuse i.e. that the wrong person will be entangled in a criminal procedure because someone has misused his or her identity (a2).

(b) Vulnerabilities also occur in the context of rule of law and fundamental rights, such as privacy, data protection and non-discrimination.

Second question: can biometric methods provide solutions to the vulnerabilities found?

The second question focuses on application of biometric data for the purpose of determining the identity of suspects and convicted persons. Does (further) application of biometrics provide solutions to specific vulnerabilities as identified above? From both a legal and a technical point of view, it is important to assess the potential added value of, as well as limitations to the use biometric data for ascertaining a persons' identity in the criminal justice chain.

Methods
For the purpose of this research, data have been gathered through document analysis and interviews with experts from academia as well as professionals working for various relevant agencies in the Netherlands (see Appendix 2).

3 International exchange of identification data

In the area of operational police and judicial cooperation in the EU (criminal investigation, surrender procedures, transfer of proceedings), personal data can be exchanged through various channels, depending on the phase of the criminal process. First, the police may directly exchange information of which they possess (under the authority of the public prosecutor). Second, if new evidence is to be gathered by means of coercive meth-

ods it is necessary to file a request for mutual legal assistance, which is usually drawn up by a public prosecutor. Third, the EU has adopted several instruments based on the 'principle of availability.' This principle states that within the Union restrictions to accessing and exchanging of investigative information should be minimalised as much as possible. This principle is for instance visible in the 'Prüm decision' which allows authorised investigators in one Member State access to national DNA and dactyloscopic databases in another Member State. In addition, designated competent authorities in the Member States and Europol have direct access to specific EU databases, such as the Schengen Information System (SIS) and its successor SIS-II. With regard to exchange of judicial documentation, the *European Criminal Records Information System (ECRIS)* is worth mentioning. Regardless of how criminal justice information is exchanged determining the correct identity of the persons involved is always crucial.

4 Findings

Effectiveness (vulnerability A)
The main goal of the aforementioned *Act on the Identification of Suspects, Convicts and Witnesses* (WIVVG) is to prevent identity misuse in all stages of the criminal process.

The WIVVG includes standard procedures for identification and verification during the various stages of the criminal justice process and defines both the powers and obligations of the competent authorities. Checks are standard instead of limited to situations when subjects claim that their identity has been mistaken. However, these standard checks do not apply to cases of cross-border cooperation. Here, it is still required that a victim of identity misuse takes action before the case will be investigated further, whereas fraudsters can easily escape.

It is important to notice that the WIVVG applies to *Dutch* criminal processes only. Interviewees do not have a clear picture of the extent to which it is possible to uphold the WIVVG's procedures when another Member States asks the Netherlands for assistance. Conversely, if Dutch authorities require assistance they are usually dependent on how the requested Member State carries out the identification process. If the suspect or convict does not complain, mistakes will usually not come to light.

Vulnerabilities may for instance be related to administrative and technical mistakes or inaccuracies; poor practical implementation of regulation; and the costs and effort of additional investigation. Because of a lack of (reliable) historical information correct determination of the identity of non-EU nationals is often particularly difficult. Additional investigation to determine a person's identity takes much time and capacity and is therefore mostly limited to the most serious cases. Especially travel documents are susceptible to fraud (e.g. passports issued by IS), making it necessary to apply other and additional methods of identity determination, for instance to ascertain a person's 'non-administrative' identity by means of biometrics.

In the Dutch system, the role of the independent Matching Authority is all important. The Authority ensures that institutions cannot change or delete personal data on their own behalf, it notes conflicting data and coordinates further (police) investigation if necessary to determine someone's identity. Again, thorough additional research is costly in terms of time and means and is mainly limited to more serious cases. In cross-border cases additional data must be gathered (usually through a request for mutual legal assistance) in other states in order to elucidate questions or doubts about a person's identity.

A problem that will remain, however, is that mistakes often come to light after years of investigation and are then very hard to correct. Even in the Netherlands, which has a relatively adequate system of identity determination, the system is far from impervious; let alone when it comes to international exchange.

Ascertaining a person's identity requires information from a very diverse range of sources in different Member States. In the EU, there exist no general harmonised procedural rules on the collection and use of identification information – e.g. on the use of population registries – which is a barrier to identity determination, also during criminal justice processes. Pursuing uniformity in this area is of course extremely sensitive, for historical and other reasons. However, databases such as ECRIS and SIS do set some rules for instance to identification data that must be attached to requests. However, for now complying with such rules is often optional instead of mandatory. Further harmonisation would require approximation of national procedures for personal identification data but this is difficult, also because of vulnerabilities in the context of fundamental rights.

For persons who have been unjustly involved in a criminal process (A2) systems like the SIS include complaints procedures, such as the opportunity to voluntarily provide fingerprints for reference. However, problems remain because a Member State may for instance refuse to remove a false alias from the system or fail to investigate cases of possible mistaken identity. Consequently, a person who wants his or her identification data to be corrected remains dependent on the goodwill of the requested state. An increase of cross-border exchange of identification information and further connection of different registries (law enforcement databases as well as other databases) will also increase the risk of dispersion of incorrect information and severely complicate the correction of errors. For now, an innocent person must prove within this whole array of databases that he or she is not the person sought after.

The situation could be improved by attributing authority to amend incorrect identification data to a single national institution in every Member State, for example equivalent to the Dutch Matching Authority, and by introducing obligations to periodically check the data. However, the quality of such a system would remain dependent on national efforts to guarantee that stored information is accurate and up-to-date. Other Member States as well as EU databases must trust that this is indeed the case. Ideally, applicable instruments should include incentives for both senders and receivers of personal identification information to check if the rules for data protection as well as quality criteria have been met with. Whether and how the Member States currently carry out such checks is not clear.

Rule of law (vulnerability B)
EU cooperation instruments such as the SIS and the Prüm treaty and Prüm decision exhibit vulnerabilities when it comes to the rights of suspects and convicts, since legal protection is mostly not harmonised. Member states apply very different criteria for instance for procedures regarding their biometric databases, such as time limits for keeping the data and for which offences can biometric data be gathered. The same applies to the issuing of alerts, for example regarding the criteria on which alerts must be based. However, in the current political context of the EU any attempt to harmonise such requirements might well lead to the setting of a lowest common denominator without actually improving legal protection.

At the EU level, harmonising privacy rules is on the agenda, including in the field of criminal justice (the new Privacy directive). Norms, however, are formulated in rather general terms, as is illustrated by purpose limitation rules for police investigations. In practice, the question remains how someone should find out which personal identification data is stored and in which countries and databases, now that such information can easily travel from one place to another.

Do biometric methods provide solutions to the vulnerabilities found?
The use of biometric data for identity determination may be helpful to reliable and correct identification of a person during all stages of the criminal justice chain, because it is difficult to ensure this with administrative data only, particularly further down the criminal justice chain. It is necessary to accurately determine a person's identity not only for effective criminal investigation (A1), but also for protecting the privacy of victims of identity misuse (A2). However, biometric data are not a solution in itself and combining these with administrative data remains necessary. In addition, security aspects must be taken into account because biometrics do not remedy a lack of care or a lack of alertness on the part of those who operate the system. In the Dutch system, biometric and administrative data are combined to ascertain a person's identity during the criminal justice chain. Fingerprints and photos are used only for more serious offences and in cases where when someone's identity is assumed to be incorrect. Practical experiences in the Netherlands underline the importance of biometrics but also show that well-trained and facilitated staff well-functioning equipment and procedural checks are equally crucial. An example of the latter is the requirement that those higher up in the criminal justice chain will not handle files in which the identification process has not been conducted adequately. However, no single method is fool proof and putting absolute confidence in biometric techniques holds the risk that mistakes or cases of fraud will not be detected and corrected until after a long time, or not at all.

The process of collection, processing and retention of biometric data is also vulnerable with regard to the right to privacy and the right not to be discriminated. Preventing and repairing identity misuse contributes to the protection of the private sphere of the victims of such misuse, but this is as such not a sufficient reason to allow unlimited processing and storage of biometric personal data, also given the fact that there is not always a victim of identity misuse involved. Therefore, adequate safeguards must be included, for example with regard to minors, time limits and the seriousness of the offences. For now, it remains problematic that safeguards differ greatly from one country to another despite guidance by the ECHR and the EU Court of Justice.

EU rules on purpose limitation in the context of criminal investigation are rather loosely formulated. In the Netherlands, for instance, fingerprints which have been taken for the purpose of ascertaining a suspect's or convict's identity (with the aim of countering identity misuse) are also compared with fingerprints collected at crime scenes (comparison for the purpose of identifying yet unknown suspects). This brings up questions, because the use of biometrics for the purpose of identifying an unknown suspect during a criminal investigation has its own specific vulnerabilities. The fact that someone's fingerprints have been found at a crime scene, for instance, does not necessarily imply that he or she was involved in that crime.

A loosening of purpose limitation requirements is also visible in the combining of migration and criminal law databases. It is clear that ascertaining the identity of non-EU nationals who are also suspected of a criminal offence, comes with specific challenges. There is often a lack of information which makes it difficult to effectively compare identification data, which necessitates more thorough investigation. But subjecting non-EU nationals to even further reaching powers to ascertain their identity because of this, or to use both criminal law and migration databases for this purpose, entails risks of stigmatisation and discrimination.