Introduction
Expert-based methods are used from the beginning of the 20th century for forensic evaluation of fingermarks (trace specimens) and fingerprints (reference specimens). Currently semi-automated systems using specific biometric technologies are developed to support experts in providing a more objective evaluation to the court, in terms of strength of evidence. At the same time growing data privacy concerns have enacted further legislation protecting personal data.

This study applies to the Dutch and European Union privacy and further legislation protecting personal data. At the same time growing data privacy concerns have enacted objective evaluation to the court, in terms of strength of evidence. Models are developed to support the experts in providing a more objective evaluation to the court, in terms of strength of evidence. Models are developed to support the experts in providing a more objective evaluation to the court, in terms of strength of evidence.

Problem description
The current statistical models developed for the forensic evaluation of fingermarks and fingerprints are data-driven, meaning they require the use of biometric data and metadata of a large amount of data subjects (those of whom the personal data are processed), in order to compute the strength of evidence. The study analyzes privacy and data protection issues beyond a mere compliance check in line with contemporary legislation. In addition to compliance it includes a wider understanding of privacy concerns arising when personal data are being processed for any given reason. This is performed by means of a Privacy Impact Assessment (PIA).

Privacy Impact Assessment (PIA) Methods
The PIA is a risk-analysis instrument with which privacy issues can be identified and localized. It has been designed to assist and further promote the default privacy setting of all systems used to process personal data. It fosters a win-win situation between data subjects, controllers and processors (those who need the data to perform their processing operations). It creates an environment in which processes can be operated optimally while minimizing privacy or data protection concerns.

Several Privacy Impact Assessment methods have been developed [1-5], which all have in common a number of steps:
1. Definition of contextual information regarding the particular processing operations
2. Determination of potential risks (threats and vulnerabilities) in the system or during processing regarding privacy and data protection specifically
3. Analysis and categorization of effects and risks, their impact and likelihood of occurrence
4. Risk management (necessity and relevance analysis)
5. Documentation and implementation of the PIA
6. Review and audit throughout the entire personal data lifecycle.

Applications to forensic evaluation processes
1. Define the contextual information:
   a) Project specification
   b) Forensic evaluation R&D and casework processes
   c) Personal data
   d) Fingerprint/print data (biometric data)
   e) Controllers, processor and stakeholders
   f) Purpose for processing

   2. Determine the potential risks related to:
   a) Type, quality and amount of data
   b) Presence and type offingermarks, rolled inked fingerprints (the amount of data depends on the magnitude of the strength of evidence to be computed)
   c) Type of technology
   d) Computer system embedding automatic fingerprint/print feature extraction, feature comparison and forensic statistical evaluation methods
   e) Security (technical and organizational)
   f) Way of processing
   g) Consent or legal basis to collect, disseminate, exchange, retain, link and destroy data
   h) Further processing for other purposes

3. Analyze and categorize the effects and risks, their impact and likelihood of occurrence on:
   a) People
   b) Systems and processes
   c) Potential threats and vulnerabilities for the computer system and the forensic evaluation processes (casework and R&D)

4. Manage (analyze necessity and relevance of) risk through:
   a) Mitigation
   b) Minimization
   c) Acceptance

5. Document and implement the PIA by:
   a) Publishing a descriptive document of all the steps performed above (without disclosing security-sensitive information)
   b) Communicating the PIA to all stakeholders and Data Protection Authority (DPA) / Data Protection Officer (DPO)
   c) Using a PIA to install privacy consistent processing operations

6. Review and audit throughout the entire personal data lifecycle:
   a) By checking periodically the practical implementation
   b) Whenever changes or additions in processes occur

Recommendations
Processing fingerprint/print data is part of the core business of a forensic service provider. It is important that they are processed in an environment and manner that respects informational privacy. At the same time it should not adversely effect the validity and reliability of the forensic fingerprint/print evaluation methods.

The forensic service provider must simultaneously ensure protection of the data processed, chain of evidence, transparency of forensic evaluation methods used and confidentiality of casework handled. As the PIA aims at finding the right balance between all interests, there are a few issues that stand out.

It starts with accepting the inherent risks of computing the strength of evidence of fingermarks of limited quality using possibly very large amounts of fingerprints. At the same time these data can be pseudonymized, metadata can be limited and access to facilities, processes and data can be systematically controlled and logged to ensure accountability in case of breach. This balance can only be achieved if internal and external awareness and responsibility is promoted on both individual and collective levels.

After documentation of the PIA, it is up to the forensic service provider to implement the recommendations the PIA exposes. In addition, a periodic revision and reassessment of the PIA helps enhance the awareness and promotes data protection specifically, in the entire lifecycle of the fingerprint/print data, whenever changes or additions in processes occur.

Apparently the recommendations for casework and R&D processes can be dealt with concurrently. Nevertheless, it is still desirable to assess them separately, not only because the forensic service provider carries different levels of responsibility (as a processor for casework and controller for R&D), but also because the processes for processing related to different legislation. Casework and R&D are carried out by different people and require different systems for collecting, processing and retaining data.

Conclusion
We think this contribution provides a better understanding of the interaction between the three disciplines of law, forensic science and statistics regarding the issue of privacy and protection of the fingerprint/print data used for forensic evaluation.

This study could constitute a basis for the data protection policy of other biometric modalities. Although one must remain cautious to apply it considering the substantial privacy infringing difference between fingerprints and other biometric modalities [6].

Selected References
4. NORIS de beredigerorganisasie van IT-auditeuren, Privacy Impact Assessment: introductie, handbook en vragenlijst (2012), available via www.noris.nl
6. C.M. Baartmans, Data Protection of Fingermarks or Prints in Forensic Science: how fingerprint archives or prints for purposes of forensic research & development and casework should be processed by public forensic service providers (matters of law thesis Tilburg University), 2014.