Privacy impact assessment in large-scale digital forensic investigations

Bas Seyyar, Merve; Geradts, Z.J.M.H.

Published in:
Forensic Science International: Digital Investigation

DOI:
10.1016/j.fsidi.2020.200906

Publication date:
2020

Citation for published version (APA):
Bas Seyyar, M., & Geradts, Z. J. M. H. (2020). Privacy impact assessment in large-scale digital forensic investigations. *Forensic Science International: Digital Investigation*, *33*, [200906]. https://doi.org/10.1016/j.fsidi.2020.200906

Forensic Science International: Digital Investigation 33 (2020) 200906

Contents lists available at ScienceDirect

Forensic Science International: Digital Investigation

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

Privacy impact assessment in large-scale digital forensic investigations

M. Bas Seyyar [a], [b], *, Z.J.M.H. Geradts [b]

[a] University of Groningen, PO Box72, 9700 AB, Groningen, The Netherlands
[b] Netherlands Forensics Institute, Laan van Ypenburg 6, The Hague, The Netherlands

ARTICLE INFO

Article history:
Received 10 October 2019
Received in revised form
30 December 2019
Accepted 17 January 2020
Available online 18 March 2020

Keywords:
Privacy impact assessment (PIA)
Data protection impact assessment (DPIA)
Big data forensics
Privacy
Directive EU 2016/80
Police directive
Law enforcement directive
Big data
Digital forensics

ABSTRACT

The large increase in the collection of location, communication, health data etc. from seized digital devices like mobile phones, tablets, IoT devices, laptops etc. often poses serious privacy risks. To measure privacy risks, privacy impact assessments (PIA) are substantially useful tools and the Directive EU 2016/80 (Police Directive) requires their use. While much has been said about PIA methods pursuant to the Regulation EU 2016/679 (GDPR), less has been said about PIA methods pursuant to the Police Directive. Yet, little research has been done to explore and measure privacy risks that are specific to law enforcement activities which necessitate the processing of large amounts of data. This study tries to fill this gap by conducting a PIA on a big data forensic platform as a case study. This study also answers the question how a PIA should be carried out for large-scale digital forensic operations and describes the privacy risks, threats we learned from conducting it. Finally, it articulates concrete privacy measures to demonstrate compliance with the Police Directive.

1. Introduction

The personal data processing of large-scale digital evidence in criminal investigations falls within the scope of Directive (EU) 2016/680 of the European Parliament and of the Council (the so-called Police Directive). This legislative instrument has entered into force on the 5th May 2016 and repeals Council Framework Decision 2008/977/JHA. This directive not only protects individuals' personal data which are being processed for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties but also ensures a high level of public security by the free flow of such data between competent authorities. Member States were expected to transpose the directive into national law from May 2016 to May 2018 (EC & EP, 2016a).

One of the most important provisions of the directive is set out in Article 4(1) (EUR-Lex, 2017) which states that personal data of natural persons must be: *a) processed lawfully and fairly; b) collected for specified, explicit and legitimate purposes and processed only in line with these purposes; c) adequate, relevant and not excessive in relation to the purpose in which they are processed; d) accurate and updated where necessary; e) kept in a form which allows identification of the individual for no longer than is necessary for the purpose of the processing; f) appropriately secured, including protection against unauthorised or unlawful processing.* The said Article 4 stipulates that Member States shall ensure that the processing is in accordance with the principles of necessity and proportionality (EC & EP, 2016a).

The Police Directive contains various novel provisions to address the limited scope and the outdatedness of the Framework Decision (de Hert and Papakonstantinou, 2016). At first glance, data protection by design and by default are introduced in Article 20 as two of the obligations of the controller. Thus, the competent authorities must take into account these two principles *both at the time of the determination of the means for processing and at the time of the processing itself.* Another novelty is the notification of a personal data breach to the supervisory authority as stipulated in Article 30. Moreover, designation of a data protection officer is introduced in Article 32 as a new obligation for the controller. Last but not least, the directive provides new rights to data subjects which include right to receive information by the data subject (Article 13), right of

* Corresponding author. University of Groningen, PO Box72, 9700 AB, Groningen, The Netherlands.

E-mail addresses: m.bas.seyyar@step-rug.nl (M. Bas Seyyar), z.geradts@nfi.nl (Z.J.M.H. Geradts).

https://doi.org/10.1016/j.fsidi.2020.200906

access by the data subject (Article 14), and right to rectification or erasure of personal data (Article 16) (Leiser and Custers, 2019).

Whereas there has been an intense debate about the role, impact and practical implementation of the Police Directive, it is clear that the directive is a positive improvement towards a comprehensive data protection in EU (EDPS, 2015). Another interesting debate is that the right to data protection and public security seem to be as competing interests (Europol, 2018). This implementation comes against the background of a debate on how the right to data protection and the right to security can be balanced within a society where the police may at times seemingly give priority to the obligation to keep society safe over privacy and data protection. As underlined by the European Court of Human Rights' case law (Volker und Markus Schecke GbR (C-92/09), Hartmut Eifert (C-93/09) v Land Hessen, 2010), the right to the protection of personal data is not an absolute right; that is, the enjoyment of this right may be limited to ensure that other rights are protected, such as when protecting society from crime and terrorism.

What is missing from the Police Directive is the guidelines on how to successfully implement appropriate safeguards for compliance (Marquenie, 2017). One of the provisions requires data controller to carry out a Data Protection Impact Assessment (DPIA) as addressed in Article 27. DPIAs (previously known as privacy impact assessments (PIAs)) are tools to evaluate the origin, nature, particularity and severity of risks to the rights and freedoms of natural persons and to determine the appropriate measures (EC & EP, 2016b).

How member states determine whether a PIA (DPIA can to some extent be seen as a GDPR checklist and primarily focused on 'data protection' while PIA includes both the right to private life and the right to data protection. Because of its broad scope, we use the term PIA instead of the term DPIA used in the Police Directive) has to be carried out is provided in Article 27(1) as follows:*Where a type of processing, in particular, using new technologies, and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural persons, Member States shall provide for the controller to carry out, prior to the processing, an assessment of the impact of the envisaged processing operations on the protection of personal data.* Furthermore, Article 27(2) provides a minimum standard for conducting a PIA:*The assessment referred to in paragraph* 1 shall *contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address those risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Directive, taking into account the rights and legitimate interests of the data subjects and other persons concerned*(EC & EP, 2016a).

Fortunately PIAs have been studied in detail since the mid-1990s (Wadhwa and Rodrigues, 2013). There are plenty of PIA methods which are proposed by researchers, governments, Data Protection Authorities (DPAs) and standards bodies. Yet, more industry/technology-oriented PIA methods are developed, such as the RFID PIA (Spiekermann, 2012) and Smart Grid DPIA template (Smart Grid Task Force, 2012–14 Expert Group 2, 2014). However, it is not the case for the police sector. The costs of using a PIA methodology not considering the unique nature of police activities can be insufficient identification of risks and difficulty in demonstrating compliance with the Police Directive.

This paper addresses these issues by evaluating existent PIA methods, providing a comprehensive methodology for digital forensics based on hands-on experience with a particular attention to large-scale processing. This work is an important step towards a better understanding of privacy risks specific to law enforcement processing practices by establishing a baseline for the assessment and treatment of these risks. Lastly, it presents a guide to the implementation of privacy-by-design (PbD) principles in large-scale digital forensic investigations.

The remainder of the paper is structured as follows. Section 2 presents Hansken and discusses state of the art. Section 3 describes the methodology. Section 4 gives an overview of the results of the case study. Finally, Section 5 presents our conclusions and our plans for future work.

2. State of the art

Since we propose to conduct a case study on Hansken, we first give an overview of Hansken in this section.

2.1. Introduction to digital forensics as a service (DFaaS)

In this section we present Hansken and its predecessor, so-called Xiraf (an XML Information Retrieval Approach to digital Forensics).

Xiraf was developed by the Netherlands Forensic Institute (NFI) as an XML-based approach to manage and query forensic traces from the high volume of seized digital material. Xiraf executes lots of forensic analysis tools in a systematic way for extracting traces as XML-based outputs. In this way, the outputs of analysis tools are integrated in order to be indexed and queried in a centralized XML-database. Users are able to search and browse the outputs through a web interface (Alink et al., 2006). Its next version was described as a second generation forensic analysis system with new functions such as parallel execution, reduced I/O, distributed processing and more (Bhoedjang et al., 2012). Its latest version is a service based approach named DFaaS. Unlike traditional digital investigation process, the data, the software and the storage and processing capacity are centralized. So, this version provides faster forensic analysis process, sooner trace availability, reduced overhead time and central system that can used by multiple departments concurrently (van Baar et al., 2014).

Hansken is the successor of Xiraf with a capacity of processing three terabytes of data per hour. Three main reasons for developing Hansken are to minimize case lead time, maximize trace coverage and specialization of people involved. Considering the sensitivity of the processed data in such a big data platform, the developers specified eight design principles: (1) Security, (2) Privacy, (3) Transparency, (4) Multi-tenancy, (5) Future proof, (6) Data retention, (7) Reliability, (8) High availability. As a big data solution, Hadoop Distributed File System (HDFS) and Map Reduce were used. Hansken is the first large-scale digital forensic system that is implemented PbD in mind (van Beek et al., 2015).

2.2. PIAs in law enforcement and justice sectors

An attempt to draft a comprehensive PIA methodology for law enforcement agencies (LEAs) was made in an European Commission's project which is Visual Analytics for Sense-making in Criminal Intelligence Analysis (VALCRI). In their white paper, Schlehahn et al. (2014) present a comparative analysis of DPIA methodologies of five European countries which are Belgium, France, Germany, Spain and United Kingdom and the Article 29 Working Party Guidelines. Their results show that none of the compared methodologies refer to the application area of Police Directive. Also, they claim that the risk for an interference on fundamental rights always exists on law enforcement processing even if it is legally justified. No matter of which methodology chosen, PIAs should be used to minimize this interference as much as necessary and appropriate safeguards should be built into processes and systems.

In 2014, the Information Commissioner of the Republic of

Slovenia (IP RS) (IP RS, 2017) published PIA guidelines for adopting new police powers. According to the Commissioner, a PIA should be conducted for new legislative proposals dealing with police powers before entering standard legislative process, especially if these proposals have strong technological aspect(s). The guidelines lay out how to identify and manage privacy risks for adopting possibly privacy invasive technologies with a particular attention to the required analysis of the necessity, suitability, effectiveness, and proportionality of the proposal. A case study for a draft legislation is included to show how to conduct a PIA based on these guidelines. Similarly, the Dutch government developed its own PIA model for draft legislations for not only police powers but also other legal areas. This PIA model is included in the Integrated Policy and Regulatory Assessment Framework (IAK) (Dutch: Integraal Afwegingskader beleid en regelgeving). Thus, it is mandatory for the government to take the results of a PIA into account when developing new legislation (Ministerie van BZK & Ministerie van VenJ, 2017). These initiatives are not at a level of technological development itself but at a 'higher' level, at the legislation level. While one might argue that a PIA at legislation level means that the legal basis of the technological development is privacy friendly/sound, in reality, this level may not be enough and a PIA at technology level may identify different or more risks that are not immediately evident at legislation level.

3. Methodology

This paper describes how to conduct a PIA in large-scale digital forensic investigations. To this end, we conduct a case study where the big data forensic platform (the so-called DFaaS) developed by the NFI is used as an example to carry out the PIA. This big data forensic solution is called Hansken as mentioned in Section 2.1. To process and investigate multiple terabytes of seized digital material, the NFI has been using DFaaS since December 2010 (van Beek et al., 2015). The reasons for the selection of Hansken are as follows: it processes large volume of forensic data, it has built-in privacy measures for the processed data and its users (forensic investigators), transparency is one of the design principles and ranked third in terms of priority (van Beek et al., 2015).

This paper searches for examples of best practice to construct an optimal PIA methodology that best suits Police Directive requirements. For this purpose, we systematically analysed current PIA methods. The review ended in ten fundamental PIA methods: Canada Directive on PIA (Treasury Board of Canada Secretariat, 2010), CNIL (French National Commission on Informatics and Liberty) PIA Methodology (CNIL, 2017), DPIA Process under EU GDPR (Bieker et al., 2016), Dutch National Government PIA Model (Dutch PIA Model) (Dutch: Model gegevensbeschermingseffectbeoordeling rijksdienst) (Ministerie van BZK & Ministerie van VenJ, 2017), ISO 29134 (ISO, 2017), NZ OPC (New Zealand's Office of the Privacy Commissioner) PIA Toolkit (NZ OPC, 2015), OAIC (Office of the Australian Information Commissioner) PIA Guide (OAIC, 2014), PIA Framework (PIAF) (Wright, 2013), Systematic Methodology for PIAs (Oetzel and Spiekermann, 2014), UK ICO (United Kingdom's Information Commissioner's Office) COP (Conducting PIAs Code of Practice) (UK ICO, 2014). These methodologies have some similarities like containing a threshold analysis to test the necessity of PIA and threat examples; also some differences like risk identification and evaluation approaches (Vemou and Karyda, 2018).

Each method has its strengths and limitations. After a comparative analysis, we combined the best elements (strong points) of three methodologies; which are CNIL PIA method, Dutch PIA Model and ISO 29134. At a glance, we selected the PIA guidelines that have been recently proposed or updated especially after the GDPR. Since the Police Directive and the GDPR propose similar solutions in many areas (de Hert and Sajfert, 2018), we included the methods being in line with the GDPR. Vemou and Karyda (Vemou and Karyda, 2018) argued that relying on specific legal frameworks may limit PIAs to a compliance check instead of a comprehensive review of privacy issues of a process. Hence, the inclusion of an international standard on PIA; that is ISO/IEC 29134, contributes to mitigate such limitations.

In details, our evaluation is based on the following benchmarks of ten PIA methods:

1 Is the PIA method up-to-date?
2 Is the GDPR used as a legal basis?
3 Does the PIA method provide an automatizing tool?
4 Is a guidance on how to conduct a PIA in big data context given? Does the PIA method contain a checklist/a set of questions addressing privacy risks/threats of large-scale data processing?

Almost every DPA (or ICO) provides guidelines on the implications of big data for data protection. However, guidance for big data-specific PIA is offered only in UK PIA COP (UK ICO, 2017) and Dutch PIA Model (JenV, 2018) as shown in Table 1. Both of the supplements are based on the existing PIA methodologies, key points and experience gained with Big Data. What is more, Dutch PIA Model is predicated on not only the GDPR but also the Police Directive. It proposes similar procedures for the similar articles (or recitals) with further assistance for the exceptional circumstances in the Police Directive. Similarly, the main criterion for choosing CNIL PIA Method is that it is supported by an automated tool. Such a tool may *facilitate comparison, improve standardisation, support enterprise accountability* and ease the PIA process to implement compliance, especially in multi-jurisdictional legal environments (Tancock, 2015). Nevertheless, it is argued that none of the known PIA tools are capable of addressing emerging changes in privacy laws and bridging the knowledge gap between lawyers and engineers both of whose contributions are essential for a successful PIA (US Patent App. No. 15/459,909, 2017).

CNIL PIA consists of methodology, template and knowledge bases. Its automated tool visually assists PIA practitioners and provides practicality. Specifically, CNIL's tool is designed to aid the organizations in building compliance (CNIL, 2017), to facilitate commenting on and validating PIA-related issues and to increase stakeholder involvement. It is noteworthy that the tool itself does not automate the PIA process, instead it guides PIA steps, creates PIA report, risk overview and risk mapping automatically. Also, it is important not to focus solely on the threats stated in the guideline. ISO 29134 adapted a checklist approach. Referring to other ISO standards (e.g., ISO/IEC 29151, ISO/IEC 27002) in several articles might cause PIA practitioners to loose time as it might be hard to follow. Dutch PIA Model has seventeen points explained in details for performing a PIA and a big data-specific supplement. It is a problem that there is no English translation at the moment since it is produced for proposed regulations and data processing by the government.

4. Results and discussion

This study seeks to understand de facto privacy risks in a centralized forensic platform processing large amounts of personal data. So, the privacy risks which are solely specific to Hansken and the processing of the NFI are irrelevant and beyond the scope of this paper. Instead we generalize our findings to other similar platforms. Likewise, we do not evaluate the privacy risks since they are dependent on the priorities and risk criteria of LEAs.

It should be noted that the processing of the NFI falls in reality under the GDPR. This is because the Ministry of Justice and Security

Table 1
Comparative analysis between PIA methods.

PIA Methods	Release Date OR Latest Update	Legal Framework	Automated PIA	Big Data Support
Canada Directive on PIA	2010	Canada's Privacy Act 1985	×	×
CNIL PIA Methodology	2018	GDPR	✓	×
DPIA Process under EU GDPR	2016	GDPR	×	×
Dutch PIA Model	2017	GDPR & Police Directive	×	✓
ISO 29134	2017	×	×	×
New Zealand PIA Toolkit	2015	New Zealand's Privacy Act 1993	×	×
OAIC PIA Guide	2014	Australia's Privacy Act 1988	×	×
PIAF	2013	×	×	×
Systematic Methodology for PIAs	2014	×	×	×
UK PIA COP	2014	UK's Data Protection Act 1998	×	✓

has no independent powers for the prevention, investigation, detection and prosecution of indictable offences or the enforcement of punishments and no link can be made with the “competent authority” as stated in the Directive. However, the forensic investigations in the majority of the member states (e.g., France, Belgium, Spain) are performed by a police unit and the aforementioned processings fall under the Police Directive. Therefore, we limit our case study to the Police Directive.

4.1. General description of the envisaged processing operations

Hansken processes special categories of personal data and personal data relating to criminal convictions and offences on a large scale. This processing is likely to result in high risk to the rights and freedoms of natural persons. Also, an amendment of the Police Data Act (Dutch: Wet politiegegevens (Wpg)) and the Judicial and Criminal Records Act (Dutch: Wet justitiële gegevens (Wjsg)) to implement the Police Directive has entered into force on January 1, 2019 after DFaaS has become a standard for criminal cases (December 2010) (Decree implementing the Directive data protection investigation and prosecution, 2019). The processing within Hansken is expected to be in conformity with these new provisions. For these reasons, a PIA should be carried out.

The NFI developed Hansken as a digital search engine for processing and investigating high volumes of (seized) digital material. Its goal is to give the right people access to the right information at the right time. With Hansken, an investigator can quickly and efficiently search for traces in large quantities of seized data carriers such as computers and mobile phones. Anything that may be relevant can be searched for, for example words and names or properties of traces such as chat-messages, emails or photos, whether or not taken with a certain camera. Its processing provides a significant contribution towards finding the truth in criminal cases.

Hansken is used for case investigations on request and under the direction of the police and the Public Prosecution Service (PPS) (Dutch: Openbaar Ministerie (OM)). For this task, the NFI, the police and the PPS are considered as joint controllers. The data for this task are supplied by the police and/or other investigative authorities. Other usages are development of libraries and software and giving courses on how to use Hansken. For these tasks, the NFI is considered as the controller. These core tasks fall under Regulation of the Minister of Security and Justice, dated 8 May 2012, no. 227774, containing provisions regarding the assignment of the NFI (Regulation of NFI duties) (Regeling taken NFI, 2012).

Possible data subjects are convict(s), suspect(s), victim(s), witness(es) and third parties who have nothing to do with the investigation, or persons who are wrongly suspected. With Hansken, all categories of personal data can be processed. For example, information from a mobile telephone contains among other things photograph, names, phone numbers, e-mails, meta-data, location data, payment data, video, data concerning religious conceptions or health etc. Thus, the processing can therefore concern common personal data and sensitive personal data (Recital 37 of the Police Directive (EC & EP, 2016a)). The persons who access the case data are officials from Hansken team.

Within Hansken framework, there is a wide variety of supporting assets, ranging from forensic analysis tools to big data solutions. The forensic tools collection consists of existing forensic tools, both publicly available tools such as UFED, EnCase, FTK, EXIF etc. and tools that is developed in-house. HDFS, Map Reduce, Cassandra, HBase, Elastic Search, Kafka are some of the modules/components used in DFaaS architecture. Discussing all these assets in detail goes beyond the scope of this paper.

Strategies for privacy and security are based on the commandments from the Jericho Forum. The Jericho Forum consisting of IT customers and vendor organisations proposes a new security model called de-perimeterisation instead of central protection (Lacey, 2005). The goal of de-perimeterisation is to make information flows boundaryless by using encryption, inherently secure computer protocols, inherently secure computer systems and data level authentication (van Beek et al., 2015). Apart from that, role-based access control (RBAC) is used for identity and user management. With RBAC, access rights are linked to roles within the organization or business process. System users obtain access rights by fulfilling a certain role.

Once the data are read from the seized material, it becomes encrypted. Stored data are encrypted too. The encryption keys are stored in a different domain and separated from the encrypted image. All requests to the central service like authentication, authorization, data uploads, forensic queries, content retrievals are logged. Any privacy-sensitive information in log messages is removed by replacing identifying (tagged) information with anonymized (irreversible) or deidentified (reversible) values. To reverse deidentified values, access to the cryptographic keys is required. Hansken uses HDFS which ensures data availability with three replicas per file by default. Additionally, Hansken works on a copy of the seized material, so the original data are still available for recovery.

Indexing and analysing high volume of seized digital material are main interests for Hansken's usage. These usages are necessary, otherwise searching for traces would be time consuming and detection capacity would be scarce. Based on the data processed by Hansken, no automated decisions producing legal effects for the people concerned or significantly affects him or her, are taken. Final decisions regarding data subjects are always taken with human intervention (the investigator or the examining magistrate).

Statutory protected categories of data (e.g., correspondence between lawyers and/or doctors and their clients, hereafter referred to as 'confidentiality communication') should be protected from being disclosed in criminal proceedings as stated in Code of Criminal Procedure (Dutch: Wetboek van Strafvordering (WvSv), Article 126aa(2)). Within Hansken there is a *tool* to exclude confidentiality communication. That tool works as follows: The defence lawyer provides a list of keywords, files, folders etc. that are highly likely to contain confidentiality communication. The traces having one or more hits according to the list are given the status 'marked' (suspected). Furthermore, when someone investigating data in Hansken encounters suspected confidentiality communication, he/she gives the trace the status 'marked' too. An assessor, an employee who is not involved in the investigation and has specific authorizations, then decides whether confidentiality communication is indeed involved. If that is the case, the trace is given the status 'confirmed'. If there is no confidentiality communication, the trace will receive the status "rejected". For Hansken users such as the investigators, only the traces with the status 'unmarked' and 'rejected' can be requested (ECLI: Netherlands: RBAMS: 2018:2504). The functionality of this tool is in compliance with the instruction manual adopted by National Assembly Investigation Officers (National Assembly Investigation Officers (Dutch. Landelijke Vergadering Rechercheofficieren), 2014).

Hansken may be used for profiling the suspects. For instance, location and behavioural characteristics of a suspect can be determined on the basis of the digital evidences. Algorithms and techniques used in Hansken have been scientifically tested, as shown in publications or peer reviews. Some of them are publicly available like firearm detection and geodata extraction algorithms. The others are not released publicly because this can potentially harm the detection process. However, insight might be given to the defence as to how the data have been processed in a certain case, as allowed by the examining magistrate. Hansken uses big data: by using large amounts of structured and unstructured data from different sources, data are analysed to look for traces and correlations that can provide knowledge for investigations.

Regulation of NFI duties, Criminal Experts Act (Dutch: Besluit register deskundige in strafzaken (DIS)), Code of Criminal Procedure (WvSv), conventions such as the Prüm Treaty and International Legal Assistance Convention (Dutch: Internationale Rechtshulpverdragen) provide the necessary legal grounds for the processing within Hansken. In addition, in the Ennetcom-case (ECLI: Netherlands: RBAMS: 2018:2504), the court ruled that the results obtained from Hansken are not unreliable, that the procedures have been sufficiently controllable by the defence and that the use of such helps does not require any additional legal provisions. The obligation for the NFI to process personal data may, if appropriate, arise from Criminal Experts Act. On the basis of this law, experts of the NFI can receive instructions for carrying out an expert investigation from the examining magistrate or the public prosecutor. The personal data are not processed for another purpose then for which it has been collected, namely for the detection of criminal offences. Personal data from a specific case are not combined with personal data from another case, unless the PPS has given specific permission to the NFI.

Having access to and being able to analyse large amount of data are crucial in the process of truth-finding. For analysing such large volume of forensic data within a reasonable time, there is no less intrusive way than using Hansken. Therefore, it can be judged that the means are proportionate to the legitimate aim pursued. Furthermore, the processing purposes cannot be achieved if fewer data were processed in Hansken. For finding the truth in (criminal) cases it is of great importance that not too little data are collected, because precisely as complete a picture as possible has to be created of a situation/suspect, also to relieve the suspect. A relevant research question can be for example: Does X appear in the file? Such a question can only be answered by searching through all available material. All data processed in Hansken are necessary for achieving the goal, precisely because links are sought in a process that can serve as evidence. It is not always possible to determine in advance which/what type of data and which person is involved. In that sense, "data minimization" cannot be met.

The NFI has been accredited by the Dutch Accreditation Council in a number of fields based on EN ISO 15189:2012, EN ISO/IEC 17025:2005, EN ISO/IEC 17020:2012 (Dutch Accreditation Council, 2019) and complies with The National Government Information Security Baseline 2017 (Dutch: Baseline Informatiebeveiliging Rijksdienst (BIR)) according to the "comply or explain" principle.

4.2. *Assessment of the risks to the rights and freedoms of data subjects*

The privacy risks specified in this section are in line with CNIL PIA Methodology and ISO 29134 (CNIL, 2017; ISO, 2017).

4.2.1. *Illegitimate access to data*

Illegitimate access may lead to considerable damages to the data subjects due to the amount and privacy sensitivity of the data such as discrimination, damage to reputation, financial loss etc. Further, any unauthorised disclosure may have a negative influence on the discovery of truth in criminal investigations. For instance, a situation where a suspect finds out by means of an unauthorized access that he/she is under secret investigation may frustrate the investigation.

Some main threats that can lead to an illegitimate access are as follows: (1) Data process/read for wrong case. (2) Unencrypted data transmission from third parties. (3) Unauthorized person access to the big data forensic platform. (4) Investigation report (paper documents) sent to wrong destination. (5) Access to data after case is closed. (6) No systematic monitoring of authorizations. (7) Illegitimate cross-referencing of data (ISO, 2017).

4.2.2. *Unwanted change of data*

Unwanted change of data may cause the big data forensic platform to fail to operate correctly. Also, the processing could be misused for evidence manipulation; a piece of evidence might be altered in other valid data such as data about location or movements, economic situation, etc. As a result, there might be occasions where someone commits a crime and an innocent person is accused of it and personal data are processed in a manner that is incompatible with specified and legitimate purposes.

Some main threats that can lead to unwanted change of data access are as follows: (1) Errors during updates, configuration or maintenance (ISO, 2017). (2) Malicious code injection (CNIL, 2017). (3) Replacement of an original document (paper) by a forgery (ISO, 2017). (4) Replacement of components (ISO, 2017). (5) Authorizations not granted at case level. (6) Not to ensure separation of duties (e.g., between system administrators, operators and investigators). (7) Errors while uploading seized digital material. (8) Insufficient knowledge of the software.

4.2.3. *Disappearance of data*

Disappearance of data may dramatically effect data availability. In digital investigations, data availability should be high, preferably 24/7, otherwise the amount of evidence found in digital material will decrease and time needed to solve a case will increase (van Beek et al., 2015). Like unwanted change of data, data disappearance may cause to malfunction. In consequence, the outcomes of these feared events may produce adverse legal effects concerning the data subject.

Some main threats that can lead to disappearance of data are as follows: (1) Processing capacity overload (ISO, 2017). (2) Denial of service attack (CNIL, 2017). (3) Ageing of archived documents (CNIL, 2017). (4) Loss of encryption key. (5) Assignment of poorly trained employees. (6) Under tested software/hardware integration.

4.3. The measures envisaged to address the risks

In this section, we discuss appropriate measures for a big data forensic platform, as summarised in Table 2, to address the privacy risks identified in the previous section.

1 Access to the platform should be permitted only to personnel who possess a security clearance.
2 If an investigator is no longer working on a case, his/her access to the case data should be immediately withdrawn.
3 LEAs should impose strict data retention periods in accordance with the requirements of all applicable legislation. In case of a need for longer retention periods, the data should be anonymized. Also, specifications on how to destroy the personal data in a secure manner should be developed. Procedural measures have to be in place to ensure retention and destroy policies are respected.
4 Case data and queries made by investigators for searching traces should be kept encrypted.
5 Software used in the platform especially forensic analysis tools should be analysed with regard to privacy.
6 Confidentiality communication (e.g., information covered by legal professional privilege) should be excluded as evidence for criminal prosecution. Unfortunately, there does not exist a forensically sound procedure that is able to guarantee the protection of confidentiality communication and current practices require manual intervention (Jiang et al., 2013). Hence, the disclosure of such information should, as far as possible, be protected. To this end, a list of keywords to filter out the relating privileged data might be specified in advance. The defence lawyer might be consulted for specifying the possible keywords. Search for these keywords should only be allowed with prior justification (Naudts, 2018). It is possible that the traces are not correctly recognized as privileged and not filtered out during the investigation. In this case, an investigator might mark traces as privileged and filter them out immediately. Likewise, it is also possible that some data are incorrectly classified as privileged. In this case, an officer being not involved in the investigation may be designated and he/she may restore non-privileged data.
7 To reduce the risk impact, it should be ensured that any disclosure of personal data is detected as soon as possible

Table 2
Summary of threats, privacy risks, measures to address the risks and related provisions in the Police Directive (* Recital, ** Article).

Examples of Threats	Privacy Risks	Measures	Provisions
	Illegitimate access to data	1	Best Practice
1		2	Rec.* 37
Data process/read for wrong case.		3	Rec. 26,41,42; <
			Art. ** 5,20(2),22(3d),29(c)
2		4	Art. 29(b)
Unencrypted data transmission from third parties.		5	Best Practice
		6	Best Practice
3		7	Art.30
Unauthorized person access to the big data forensic platform.		8	Rec. 26
		9	Rec.37; Art.29(a)(e)
4		10	Rec. 57, 96; Art.25
Investigation report (paper documents) sent to wrong destination.		11	Art.29(e)
		14	Rec 31; Art.6
5		16	Best Practice
Access to data after case is closed.			
6			
No systematic monitoring of authorizations.			
7			
Illegitimate cross-referencing of data			
1 Errors during updates, configuration or maintenance	Unwanted change of data	1	Best Practice
2 Malicious code injection		2	Rec. 37
3 Replacement of an original document (paper) by a forgery		3	Rec. 26,41,42;
4 Replacement of components			Art. 5,20(2),22(3d),29(c)
5 Authorizations not granted at case level		5	Best Practice
6 Not to ensure separation of duties		9	Rec.37; Art.29(a)(e)
7 Errors while uploading seized digital material		10	Rec. 57, 96; Art.25
8 Insufficient knowledge of the software		11	Art.29(e)
		12	Rec. 33,96; Art. 29(j)
		13	Rec.30, Art.7(2)(3),16(3a)
		16	Best Practice
1 Processing capacity overload	Disappearance of data	1	Best Practice
2 Denial of service attack		2	Rec. 37
3 Ageing of archived documents		5	Best Practice
4 Loss of encryption key		9	Rec.37; Art.29(a)(e)
5 Assignment of poorly trained employees.		10	Rec. 57, 96; Art.25
6 Under tested software/hardware integration		11	Art.29(e)
		12	Rec. 33,96; Art. 29(j)
		16	Best Practice

and supervisory authority (e.g., PPS or DPA) is informed accordingly.

8 Datasets used for training and software testing should be anonymized.

9 Strict access control policies should be in place to limit the risk of unauthorised access to personal data.

10 Any user/system actions should be logged, attributed to diagnose any privacy breaches and to preserve the chain of evidence. Article 25 of the Police Directive sets out how detailed the logs should be as follows: *the justification, date and time of such operations and, as far as possible, the identification of the person who consulted or disclosed personal data, and the identity of the recipients of such personal data.* The said article also limits the usage of logs. To protect the privacy of employees, logs might be pseudonymised too.

11 To implement the principle of purpose limitation, the big data forensic platform should keep an explicit audit trail of user actions. Audit trails may verify that the actions of the forensic investigator are within the scope of a warrant/court order and also reinforce the evidence reliability (Adams, 2008). To achieve a higher-level of auditing, *unique user profiles which are tied to individual analysts and allow for varying degrees of access to data based on the tasks assigned and clearance given* may be provided (Marquenie and Coudert, 2017).

12 It is important that the case data (seized digital material) are handled meticulously and carefully throughout the entire investigation: both when collecting data from third parties and when transferring it to the platform. The original digital material should be kept outside of the platform's processing, an exact copy should be made and used for searching traces. To monitor its integrity and minimize the errors, a hash function and a message authentication code (MAC) could be used.

13 To ensure data accuracy, the data must be categorized according to its reliability. For this purpose, 4x4x4 (Belgium) or 5x5x5 (UK) grid structures could be used as an example. For instance, in UK 's structure (College of Policing, 2019), the data are described in 5 categories as follows: (A) Known directly to the source, (B) Known indirectly to the source but corroborated, (C) Known indirectly to the source, (D) Not known, (E) Suspected to be false (Marquenie and Coudert, 2017). By the same token, it is desirable to clearly distinguish primary data sources (the sources where data are actually generated) from secondary ones (sources that link existing data sets and (re)use them) (JenV, 2018).

14 A distinction between different categories of data subjects should be drawn. The personal data of convicts, suspects, victims, witnesses and third parties should be treated differently as addressed in Article 6 of the Police Directive. For instance, different degree of anonymization (e.g., irreversible or de-identified (reversible)) may be used for different categories of data subjects.

15 The potential discriminatory factors (e.g., the training data, the learning algorithm etc.) should be tested whether they create biases for natural persons (especially for profiling). If so, they shall be prohibited.

16 Algorithms and techniques which are scientifically derived and proven should be used in the platform. The margin of error associated with them should be determined by taking into account their potential impact on the natural persons (JenV, 2018).

17 Competent authorities could be encouraged in publishing their PIA reports (executive summary) on a publicly available platform.

4.3.1. *Discussion of principles relating to processing of personal data in law enforcement sector*

The processing of personal data in a big data forensic platform is not transparent. The data subjects such as suspects do not always know if and how their personal data are being processed. So, they cannot be asked to give their consent to the processing. They also lack insight into the accuracy and completeness of their personal data. The personal data of the persons who have nothing to do with the criminal investigation might also be processed in such a platform. These persons are not able to make use of their rights under Police Directive. It is actually impracticable for the competent authorities to be transparent about data processing of natural persons, as this involves a disproportionate amount of time and effort and the process of truth-finding may be frustrated. Since it is difficult to determine in advance which information is relevant to the case and which is not, data minimization might not be implemented in the criminal investigations.

Because the persons involved are often unable to exercise some of their rights, it is of great importance that the processing in a big data forensic platform is subject to an external control/audit by the supervisory authority. Additionally, the competent authorities might provide a clear explanation concerning the use of personal data in relation to forensic investigation within the big data platform in their website and/or social media account. In this context, an explanation of how to challenge the decisions made with the help of the platform may be put on the website for future reference.

5. Conclusion

In this paper, we described how to conduct a PIA on a big data forensic platform. To this end, we compared several PIA methods and selected three that best suit our requirements, since there do not exist a PIA methodology that is in conformity with the Police Directive with a focus on law enforcement activities.

Our study demonstrates firstly the importance of conducting a PIA for all forensic platforms. Seized digital material may contain large amounts of common and sensitive personal data of everyone involved in a crime. Hence, the processing for forensic purposes is more likely to result in an interference in the fundamental rights of data subjects. PIAs may be of benefit to minimize this interference. Secondly, the findings from this study strengthen the position that privacy correlates with security. Necessary measures should also be taken to ensure the security of such forensic platforms.

This case study reveals that threats in police sector that can lead to privacy risks are rather different from those in other sectors. Collaboration between the investigators and PIA practitioners is crucial in precisely specifying these threats. The implementation of a PIA encourages privacy awareness within the investigators and the developers of a big data forensic platform. It is worth noting that PIAs should be carried out before the development of such platforms. Whenever a shift in privacy objectives takes place during the design phase, LEAs should repeat the PIA to address new privacy risks.

In future work, we plan to further investigate how to improve the implementation of PbD in large-scale digital forensic investigations without reducing the effectiveness and the speed of investigations.

Acknowledgement

The authors would like to thank Prof. Jeanne Mifsud Bonnici and Prof. Katrin Franke for their valuable comments on an earlier draft of this article, Esther van Fessem for her kind suggestions; any error or omission is however the sole responsibility of the authors.

This research was supported by Evolving Security ScienceE through Networked Technologies, Information policy And Law (Essential) Project funded under the European Union's Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie [grant agreement no 722482].

References

Adams, C.W., 2008. Legal issues pertaining to the development of digital forensic tools. In: 2008 Third International Workshop on Systematic Approaches to Digital Forensic Engineering, pp. 123–132. https://doi.org/10.1109/SADFE.2008.17.

Alink, W., Bhoedjang, R.A.F., Boncz, P.A., de Vries, A.P., 2006. XIRAF – XML-based indexing and querying for digital forensics. Digit. Invest. 3, 50–58. https://doi.org/10.1016/j.diin.2006.06.016. http://www.sciencedirect.com/science/article/pii/S1742287606000776.

van Baar, R.B., van Beek, H.M.A., van Eijk, E.J., 2014. Digital forensics as a service: a game changer. Digit. Invest. 11, S54–S62. https://doi.org/10.1016/j.diin.2014.03.007. http://www.sciencedirect.com/science/article/pii/S1742287614000127.

van Beek, H.M.A., van Eijk, E.J., van Baar, R.B., Ugen, M., Bodde, J.N.C., Siemelink, A.J., 2015. Digital forensics as a service: game on. Digit. Invest. 15, 20–38. https://doi.org/10.1016/j.diin.2015.07.004. http://www.sciencedirect.com/science/article/pii/S1742287615000857.

Bhoedjang, R., van Ballegooij, A., van Beek, H., van Schie, J., Dillema, F., van Baar, R., Ouwendijk, F., Streppel, M., 2012. Engineering an online computer forensic service. Digit. Invest. 9, 96–108. https://doi.org/10.1016/j.diin.2012.10.001. http://www.sciencedirect.com/science/article/pii/S1742287612000655.

Bieker, F., Friedewald, M., Hansen, M., Obersteller, H., Rost, M., 2016. A process for data protection impact assessment under the European general data protection regulation. In: Schiffner, S., Serna, J., Ikonomou, D., Rannenberg, K. (Eds.), Privacy Technologies and Policy. Springer International Publishing, pp. 21–37 volume 9857 of *Lecture Notes in Computer Science*. http://link.springer.com/10.1007/978-3-319-44760-5.

College of Policing, 2019. Intelligence report. https://www.app.college.police.uk/app-content/intelligence-management/intelligence-report/. (Accessed 27 June 2019).

Commission Nationale de l'Informatique et des Libertés (CNIL), 2017. Privacy Impact Assessment (PIA). https://www.cnil.fr/en/privacy-impact-assessment-pia. (Accessed 28 February 2019).

Decree implementing the Directive data protection investigation and prosecution, 2019. Stb. 2018. Amendment of the Police Data Act and the Judicial and Criminal Records Act to Implement European Regulations on the Processing of Personal Data for the Prevention, Investigation, Detection and Prosecution of Criminal Offenses or the Execution of Penalties, vol 496 (Dutch. Wijziging van de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens ter implementatie van Europese regelgeving over de verwerking van persoonsgegevens met het oog op de voorkoming, het onderzoek, de opsporing en vervolging van strafbare feiten of de tenuitvoerlegging van straffen).

Dutch Accreditation Council, 2019. All accredited bodies. https://www.rva.nl/en/search?utf8=%E2%9C%93&amp;q=Nederlands+Forensisch+Instituut&amp;commit=find+organisation&amp;type=institutions. (Accessed 19 June 2019).

EC, EP, 2016a. Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. ELI. http://data.europa.eu/eli/dir/2016/680/2016-05-04.

EC, EP, 2016b. 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) (Text with EEA relevance). ELI. http://data.europa.eu/eli/reg/2016/679/2016-05-04.

EDPS, 2015. Opinion 6/2015 - a further step towards comprehensive EU data protection: EDPS recommendations for the police and justice sectors. https://edps.europa.eu/press-publications/press-news/press-releases/2015/further-step-towards-comprehensive-eu-data_en. (Accessed 6 March 2019).

EUR-Lex, 2017. Protecting personal data when being used by police and criminal justice authorities (from 2018). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri&amp;equals;LEGISSUM:310401_3. (Accessed 18 December 2019).

Europol, 2018. Freedom and security - EDEN conference report. https://www.europol.europa.eu/sites/default/files/documents/report_of_eden_conference_freedom_and_security_2018.pdf. (Accessed 6 March 2019).

de Hert, P., Papakonstantinou, V., 2016. The new police and criminal justice data protection directive: a first analysis. New J. Eur. Criminal Law 7, 7–19. https://doi.org/10.1177/203228441600700102 https://doi.org/10.1177/203228441600700102.

de Hert, P., Sajfert, J., 2018. The role of the data protection authorities in supervising police and criminal justice authorities processing personal data. In: Brière, C., Weyembergh, A. (Eds.), The Needed Balances in EU Criminal Law. Hart Publishing, United Kingdom, pp. 243–255 urn:nbn:nl:ui:12-455e0710-2d2e-4db9-ad44-f83163f910c5.

Information Commissioner of the Republic of Slovenia (IP RS), 2014. Privacy impact assessment (PIA) guidelines for the introduction of new police powers. https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/PIA_guideliness_for_introduction_of_new_police_powers_english.pdf. (Accessed 11 April 2019).

International Organization for Standardization (ISO), 2017. Information Technology – Security Techniques – Guidelines for Privacy Impact Assessment (ISO/IEC 29134:2017).

Jiang, Z.L., Fang, J., Law, F.Y.W., Lai, P.K.Y., Ieong, R.S.C., Kwan, M.Y.K., Chow, K.P., Hui, L.C.K., Yiu, S.M., Pun, K.H., 2013. Maintaining hard disk integrity with digital legal professional privilege (LPP) data. IEEE Trans. Inf. Forensics Secur. 8, 821–828. https://doi.org/10.1109/TIFS.2013.2256784.

Lacey, D., 2005. Inventing the future – the vision of the Jericho Forum. Inf. Secur. Tech. Rep. vol 10, 186–188. https://doi.org/10.1016/j.istr.2005.10.003. http://www.sciencedirect.com/science/article/pii/S1363412705000464.

Leiser, M.R., Custers, B.H.M., 2019. The law enforcement directive: conceptual challenges of EU directive 2016/680. European Data Protection Law Review, 5, 367–378. https://openaccess.leidenuniv.nl/handle/1887/79246.

Marquenie, T., 2017. The police and criminal justice authorities directive: data protection standards and impact on the legal framework. Comput. Law Secur. Rep. 33, 324–340. https://doi.org/10.1016/j.clsr.2017.03.009. http://www.sciencedirect.com/science/article/pii/S0267364917300742.

Marquenie, T., Coudert, F., 2017. Roadmap for the operationalization of legal and privacy requirements in VALCRI analysis (VALCRI-WP-2017-010). http://valcri.org/our-content/uploads/2017/02/VALCRI-WP-2017-010-Operationalisation-Legal.pdf. (Accessed 11 April 2019).

Ministerie van, B.Z.K., Ministerie van, VenJ., 2017. Model privacy impact assessment Dutch National Government (PIA). https://www.rijksoverheid.nl/documenten/rapporten/2017/09/29/model-gegevensbeschermingseffectbeoordeling-rijksdienst-pia. (Accessed 2 July 2019) (Dutch: Model gegevensbeschermingseffectbeoordeling Rijksdienst (PIA)).

Ministerie van Justitie en Veiligheid (JenV), 2018. Explanation: big data analysis - big data model privacy impact assessment Dutch national government (PIA). https://www.rijksoverheid.nl/documenten/publicaties/2018/04/01/big-data-model-geb-rijksdienst-pia. (Accessed 28 June 2019) (Dutch: Toelichting: Big Data Analyse - Big Data Model GEB Rijksdienst (PIA)).

National Assembly Investigation Officers (Dutch Landelijke Vergadering Rechercheofficieren), 2014. Instruction Manual: Processing Confidential Information Found in Seized Items and Digital Files. (Dutch. Handleiding: Verwerking Geheimhouderinformatie Aangetroffen in Inbeslaggenomen Voorwerpen en in Digitale Bestanden). Unpublished material (available upon request).

Naudts, L., 2018. The data protection impact assessment for law enforcement agencies. https://lirias.kuleuven.be/retrieve/527499 Presentation at the 12th International Conference on Communications. (Accessed 11 April 2019). Bucharest, Romania (15 June 2018).

Oetzel, M.C., Spiekermann, S., 2014. A systematic methodology for privacy impact assessments: a design science approach. Eur. J. Inf. Syst. 23, 126–150. https://doi.org/10.1057/ejis.2013.18. https://link.springer.com/article/10.1057/ejis.2013.18.

Office of the Australian Information Commissioner (OAIC), 2014. Guide to undertaking privacy impact assessments. https://www.oaic.gov.au/resources/agencies-and-organisations/guides/guide-to-undertaking-privacy-impact-assessments.pdf. (Accessed 5 April 2019).

Office of the New Zealand Privacy Commissioner, 2015. Privacy impact assessment Toolkit.. https://www.privacy.org.nz/news-and-publications/guidance-resources/privacy-impact-assessment/. (Accessed 5 April 2019).

Regeling taken NFI, 2012. Regeling van de minister van Veiligheid en Justitie, d.d. 8 mei 2012, nr. 227774, houdende bepalingen inzake de taakopdracht van het Nederlands Forensisch Instituut. BWBR0031558.

Ritchie, S. (2017). US Patent Application No. 15/459,909.

Schlehahn, E., Marquenie, T., Kindt, E., 2014. Data Protection Impact Assessments (DPIAs) in the law enforcement sector according to Directive (EU) 2016/680 - a comparative analysis of methodologies. http://valcri.org/our-content/uploads/2018/06/VALCRI-DPIA-Guidelines-Methodological-Comparison.pdf. (Accessed 9 April 2019).

Smart Grid Task Force 2012–14 Expert Group 2, 2014. Data protection impact assessment template for Smart grid and Smart metering systems (accessed 8th March 2019). https://ec.europa.eu/energy/sites/ener/files/documents/DPIA%20template_incl%20line%20numbers.pdf.

Spiekermann, S., 2012. The RFID PIA – developed by industry, endorsed by regulators. In: Wright, D., De Hert, P. (Eds.), Privacy Impact Assessment. Springer Netherlands, Dordrecht, pp. 323–346. https://doi.org/10.1007/978-94-007-2543-0_15 https://doi.org/10.1007/978-94-007-2543-0_15.

Tancock, D., 2015. Design and Implementation of a Privacy Impact Assessment Tool. Ph.D. University of Bristol. https://ethos.bl.uk/OrderDetails.do?uin&amp;equals;uk.bl.ethos.683387.

Treasury Board of Canada Secretariat, 2010. Directive on privacy impact assessment. http://publications.gc.ca/collections/collection_2018/sct-tbs/BT39-9-2010-eng.pdf. (Accessed 28 February 2019).

United Kingdom's Information Commissioner's Office (ICO), 2014. Conducting privacy impact assessments code of practice. https://iapp.org/media/pdf/resource_center/ICO_pia-code-of-practice.pdf. (Accessed 28 February 2019).

United Kingdom's Information Commissioner's Office (ICO), 2017. Big data, artificial intelligence, machine learning and data protection. https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf. (Accessed 4 June 2019).

Vemou, K., Karyda, M., 2018. An evaluation framework for privacy impact assessment methods. MCIS 2018 Proceedings 5. https://aisel.aisnet.org/mcis2018/5.

Volker und Markus Schecke GbR (C-92/09), Hartmut Eifert (C-93/09) v Land Hessen, 2010. Charter of Fundamental Rights of the European Union - Articles 7 and 8 - Directive 95/46/EC - Interpretation of Articles 18 and 20, 2011/C 13/09.

Wadhwa, K., Rodrigues, R., 2013. Evaluating privacy impact assessments. *Innovation*. Eur. J. Soc. Sci. Res. 26, 161–180. https://doi.org/10.1080/13511610.2013.761748 https://doi.org/10.1080/13511610.2013.761748.

Wright, D., 2013. Making privacy impact assessment more effective. Inf. Soc. 29, 307–315. https://doi.org/10.1080/01972243.2013.825687 https://doi.org/10.1080/01972243.2013.825687, https://doi.org/10.1080/01972243.2013.825687.