Data Matching System in The Context of e-Audit: A Threat to Privacy?
(A Research Based On The Indonesian Legal framework)

A Thesis of Master Program in Law and Technology

Tilburg University

Eva Siregar
ANR 662163

Thesis supervisor.
Prof. dr. Bert-Jaap Koops

Second Reader.
Dr.Ir.M.H. Maurice Schellekens

TILBUREG
SEPTEMBER 2012
Table of Contents

Cover .............................................................................................................. 1
Table of contents .......................................................................................... 2
List of abbreviations ................................................................................... 3
CHAPTER 1– Introduction ............................................................................ 4
1.1 Introduction ......................................................................................... 4
1.2 Research Questions ............................................................................ 10
1.3 Methodology and Structure ................................................................ 10
CHAPTER 2– Data Matching System in the Context of e-Audit .................. 13
2.1 Introduction ......................................................................................... 13
2.2 e-Audit ................................................................................................. 13
2.3 Data matching system ......................................................................... 21
2.4 Conclusion ............................................................................................ 28
CHAPTER 3– The Threats to Privacy ............................................................ 30
3.1 Introduction ........................................................................................... 30
3.2 The concept of privacy and threats to privacy ..................................... 30
3.3 Models of threats to privacy ................................................................. 34
3.4 Conclusion ............................................................................................ 45
CHAPTER 4– Legal Analysis of the Threats to Privacy .............................. 47
4.1 Introduction ........................................................................................... 47
4.2 The Indonesian legal framework ......................................................... 47
4.2.1 General ............................................................................................ 47
4.2.2 Regulation of privacy ..................................................................... 50
4.3 Lessons from the EU ........................................................................... 58
4.4 Conclusion ............................................................................................ 62
CHAPTER 5– Conclusion and Recommendations ..................................... 64
5.1 Introduction........................................................................................... 64
5.2 Conclusion ........................................................................................... 64
5.3 Recommendations ................................................................................ 66
Bibliography ................................................................................................. 68
## LIST OF ABBREVIATIONS

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>APEC</td>
<td>Asia-Pacific Economic Cooperation</td>
</tr>
<tr>
<td>ASOSAI</td>
<td>Asian Organization of Supreme Audit Institutions</td>
</tr>
<tr>
<td>BPK RI</td>
<td>Badan Pemeriksa Keuangan Republik Indonesia (The Audit Board of The Republic of Indonesia)</td>
</tr>
<tr>
<td>CCTV</td>
<td>Closed-Circuit Television</td>
</tr>
<tr>
<td>EDPS</td>
<td>European Data Protection Supervisor</td>
</tr>
<tr>
<td>ETL</td>
<td>Extract, Transform, Load</td>
</tr>
<tr>
<td>EUROSAI</td>
<td>European Organisation of Supreme Audit Institutions</td>
</tr>
<tr>
<td>GAO</td>
<td>General Accounting Office</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Hypertext Transfer Protocol Secure</td>
</tr>
<tr>
<td>ICT</td>
<td>Information Communication Technology</td>
</tr>
<tr>
<td>INTOSAI</td>
<td>International Organization of Supreme Audit Institutions</td>
</tr>
<tr>
<td>IPO</td>
<td>Input-Process-Output</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>OECD</td>
<td>Organisation for Economic Co-operation and Development</td>
</tr>
<tr>
<td>PSI</td>
<td>Public Sector Information</td>
</tr>
<tr>
<td>PSP</td>
<td>Pernyataan Standar Pemeriksaan (The Statement of The Auditing Standard)</td>
</tr>
<tr>
<td>SOP</td>
<td>Standard Operational Procedure</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Socket Layer</td>
</tr>
</tbody>
</table>
CHAPTER 1—Introduction

1.1 Introduction

Nowadays, information technologies have penetrated into our daily life. Like or dislike, people have to keep in pace with these kinds of technologies. The involvement of information technologies in households, private sectors, and public bodies is triggered by the efficiency and the effectivity provided by these kinds of technologies.

The invasion of information technologies affects the types of the data that are being processed. In recent years, personal data have a tendency not longer become an “exclusive data” that can only be processed by limited parties. The spreading of personal data from public bodies until private sectors proves that the information technologies give their contributions to expand the utilization of personal data.

In public sectors, the issue of good governance has challenged public bodies to improve their services in front of the public. For this reason, most of the governments all over the world have implemented e-government into their programs.¹ However, to support these programs, the governments not only require public data, but also personal data. Taxation and census programs are the examples that the government agencies process personal data.

Handling personal information is not a trivial issue considering personal information is a part of privacy that reflects dignity, respect, and integrity of individuals.² Therefore, personal information must be protected, and there should be a clear mechanism how public bodies process personal information lawfully and legitimately. The lack of sufficient legal framework to regulate how public bodies process personal information will inevitably lead to privacy concerns.

The Audit Board of The Republic of Indonesia (hereinafter “the Audit Board) as a state finance audit institution³ realizes its significant contribution in realizing good governance in Indonesia. Therefore, the Audit Board introduced a product of the development of information technology, namely “the Audit Board’s synergy”,⁴ through “an electronic audit (e-Audit) strategy” in 2009.⁵

¹ According to Darel M. West, ninety-six percent of the governments’ websites provide access to public data. As cited on July 14, 2012.  
³ Undang-undang Dasar 1945 (The 1945 Constitution) is a Constitution in Indonesia, and as a standard for other regulations in Indonesia. The Third Amendment of 1945 Constitution of The Republic of Indonesia, Chapter VIII A article 23E (1): “for the purpose of auditing financial management and accountability, a free and independent Audit Board shall be established,” 5 Feb. 2012.  
⁴ The Audit Board synergy is a concept, suggested by the Audit Board in order to improve monitoring system in management and accountability of public finances. <Hadi Poernomo. “Impact of Technology on Public Finance and Governance.”>
Implementing “the Audit Board’s synergy” through e-Audit will not only make the audit process more efficient and effective, but could also reduce the high level of corruption in Indonesia. According to a research conducted by The World Audit, Indonesia ranked 77th for corruption in 2011 out of 180 countries in the world. Therefore, implementing e-Audit would broaden the scope of an audit and increase the numbers of entities that can be audited.

The e-Audit is built by connecting e-BPK and e-Auditees through an online communication. The main objective of this connection is to “improve monitoring over public finance management and accountability in Indonesia.” Besides, this connection builds “a data center of management and accountability of public finances” and is also complemented by a mechanism of the “link and match” system.

In e-Audit, data matching system will contribute more than the “link” process, because the “link” process merely functions as a communicator. Meanwhile, the data matching system supported by the software and the hardware of the computer system has the abilities to analyze and to match the various types of the audit data.

In addition, it should be noted here that the Audit Board does not merely process public documents from the audited entities. Considering its authority in auditing the state finances, the Audit Board enables to process personal data. The Audit Board’s press release on December 23, 2011 concerning the advanced investigative audit on the Century Bank, Development In Strengthening Public Accountability and Transparency: The Audit Board of The Republic of Indonesia’s Experience (Sub Theme 2: The Challenges for Ensuring Transparency and Accountability in Specific Areas of Public Financial Management). Launch of ASOSAI &EUROSAI 1st Joint Conference. Istanbul. 22-24 September 2011. Reading: 3>.

Ibid., 3.
6World Audit is in an international not-for-profit company, registered in England by the registered charity, World Concern. As cited on August 26, 2012.
7e-BPK is the Audit Board’s information system. Meanwhile, the word ‘BPK’, stands for “Badan Pemeriksa Keuangan.” It is the abbreviation from the Audit Board in Indonesian.
8e-Auditees are the auditees’ information system. Auditees or entities are the government institutions that manage state finances. Therefore, based on Undang-undang Nomor 15 Tahun 2004 tentang Pemeriksaan Pengelolaan dan Tanggung jawab Keuangan Negara <Law Number 15 Year 2004 concerning Audit on Management and Accountability of State Finances> article 1 (4), they must be audited by the Audit Board.
9Poernomo,3.
10Ibid.
11Ibid.
12Ibid., 1.
13In this research, the data matching system uses the approach of the IPO model (Input-Process-Output) <http://en.wikipedia.org/wiki/IPO_Model>. As cited on July 14, 2012.
14The input phase: discusses the resources that are used in the data matching system, particularly the data from the audited entities. Next, the process phase: describes how the matching process is operated in BPK’s data center, and how the three subcomponents in BPK’s data center participate in the matching process. The last phase is the output: consists of profiles that could be personal profiles and/or organizational profiles.
particularly for the investigative audit,\textsuperscript{15} proved that the Audit Board also processed personal data.

Article 10 point (a) Law Number 15 Year 2004, concerning Audit on Management and Accountability of State Finances, allows the Audit Board to process the documents of audited entities and of parties related to the audited entities within the context of state finance management. This means the auditors are able to process the documents of both audited entities and third parties.\textsuperscript{16}

As a description, the Audit Board’s press release on December 23, 2011 announced that in their investigative audit report, the Audit Board revealed several unfair financial transactions and stated the initials of the parties involved.\textsuperscript{17} Generally, individuals who are implicated in corruption and bribery cases on a national level are easily recognised parties who are well-known to the public. They may be the ‘key persons’ in an organization, politicians and public officials. Therefore, in the Century Bank case, even though the Audit Board used initials to describe the implicated parties in their investigative audit report, the public could easily recognize them.

This is proved by national press statements in Indonesia, as well as online and offline news reports that disclosed the identities of the initials that appeared in the audit report by mentioning the complete names and positions of the parties implicated in the advanced Century Bank case.\textsuperscript{18} Consequently, if personal data used to support an audit report are not up-to-date and possibly inaccurate, and the initials of implicated parties are mentioned in the audit report and discussed widely in public, this could represent not only an inconvenience, but could actually damage reputations, those of both the suspects and their families.

Therefore, similarly to other products of computerized technologies; the data matching system in the context of e-Audit, not only provides the convenience and speed, but also

\textsuperscript{15}Law Number 15 Year 2004, article 13 states that the investigative audit is an audit conducted to reveal the indications of public loss and/or the elements of criminal act in the context of state finance management. As cited on July 14, 2012.

\textsuperscript{16}Third parties could be the customers of a bank, private sectors or the state/local-owned enterprises that have relation to the related audit or those that assist the audited entities in performing their projects. For instance, if an audited entity has a project to build a school, so the third parties are the developers.

\textsuperscript{17}Law Number 15 Year 2004, article 19 (1) states that the audit reports that have been submitted to the House of Representatives can be disclosed to the public. Further in article 19 (2): it is excluded for the audit reports that contain the state confidentiality. As cited on August 23, 2012.

\textsuperscript{18}<http://www.bpk.go.id/web/?p=11286> As cited on July 14, 2012. In addition, based on Law Number 15 Year 2004 article 4 (1) puts the obligation to the Audit Board to perform financial audit, performance audit, and special purpose audit. According to the elucidation of Law Number 15 Year 2004, the investigative audit is a part of the performance audit. As cited on July 14, 2012.

Advanced investigative audit report, the Audit Board reported there were discovered cash flow from several companies to personal account of parties that implicated to this case. As cited on August 23, 2012. In addition, based on Law Number 15 Year 2004 article 4 (1) puts the obligation to the Audit Board to perform financial audit, performance audit, and special purpose audit. According to the elucidation of Law Number 15 Year 2004, the investigative audit is a part of the performance audit. As cited on August 23, 2012.
threats to privacy sphere. For instance, the re-using of personal data among public bodies may represent a challenge to privacy, remembering that the speed with which personal data are spread among public bodies makes it difficult for data owners to control their personal data. Besides, the convenience and the speed will gradually reduce the involvement of human beings in analysing the data. Conversely, a complete personal profile as the output of the data matching system challenges “to construct new knowledge” of individuals through profiling.

Profiling is generated by the existence of algorithms in the matching process that contributes to automatically revealing the details of personal information. This automation makes it possible to grasp all personal data that bear relation to one another. The output of the data matching system results in a personal profile, thus facilitating the construction of new knowledge.

My concern here is that personal profiles could provide auditors with suggestions that lead to a premature description of certain individuals. This is the case, for instance, if personal profiles suggest that a certain individual spends an amount of money every month that exceeds the amount of his income. This may cause an auditor to suppose that this person has a strong motive to commit fraud. Moreover, the obligation upon auditors to apply “professional skepticism” when making judgements could cause them to analyze profiles in too much depth or beyond the context of the related audit.

Privacy issues may arise because the absence of consent and being informed means that the data owner has no control over his personal data. There are two reasons for this: he does not know that his personal data are being profiled, nor does he know the purposes or uses to which his profile is being put.

Hence, it should be emphasised that the re-use of personal data, the existence of algorithms for the automation process and the stipulation that auditors apply (professional) judgement, in combination with failing to obtain the data-owners’ consent and provide them with information on the data-matching system are potential risks for the quality of data that could damage a person’s reputation.

Therefore, Hildebrandt (2006) states that “privacy is something of value, which is worthy of protection if violated.” For this reason, one of the indicators suggesting there is a threat to privacy violation is when the individuals lack control over their personal information,

20 Professional judgement is “circumstantial based and not every auditor is expected to be competent for every assignment.” Professional judgement can be improved through training, skill and experience. <http://pakaccountants.com/profession-judgement-and-professional-skepticism-difference-in-application/>.
As cited on September 9, 2012.
because of the absence of a guarantee that the data owner has rights to control his personal information.

Further, Greenleaf’s (2011) analogy claims that like copyright, data privacy also consists of a bundle of rights. This means, if the data matching system causes the individuals to lose control on their personal information, it is the same as the condition where the individuals lose their rights to control their property. However, it should be noted that if the individuals lose their property, there is still a chance that they will get their property back. It is different from the privacy, because “once lost, it is gone forever, you can’t get it back.”

Thus, with regard to the Audit Board’s authority in processing personal data under legitimate grounds, it is not exaggerated to state that the Audit Board is one of the potential public bodies that have chances for privacy intrusion. Most of us know that privacy is not an absolute right. For reasons of public interests, the application of privacy in practice could be more flexible, but it does not mean that privacy loses its power, considering in a democratic society, privacy is protected by the law. Therefore, a “mutual respect” is required.

Consequently, a comprehensive legal regime must be stipulated in order to respond the threats to privacy, because of the invasion of the information technologies, particularly through a data matching system.

Nevertheless, every country has its own perceptions of privacy. How the Indonesian perceives the concept privacy is different from how the European does. Social and cultural factors influence a country to define a threat to privacy. As the consequences, how sufficient the Indonesian legal regime accommodates the threats to privacy because of the data matching system in e-Audit, will depend on the way how the Indonesian perceives the concept of privacy.

---

24Law Number 15 Year 2004 article 10 (a) and (b) and Undang-undang 15 Tahun 2006 <Law Number 15 Year 2006 concerning the Audit Board> article 9 (1) point “b”, “d”, and article 9 (2), give the authority to the Audit Board to access and to choose data and information that have relations to state finance management from parties who manage public finances and other parties that have relation to the audit, and the partners of the parties that spend public finances in a project (third parties). These data and information only can be used for the audit purpose. <my own translation>.
25Hildebrandt, Privacy and Identity 4.
26Foran, 1999.
27Ibid.
28Ibid.
30Ibid.
I believe for the time being, data matching system in the context of e-Audit is only designed to match general financial transactions. However, public demand on transparency and the audit report on the Century Bank case have proven to us that the Audit Board constitutes one of the public bodies that have potential to deal a lot with the processing of personal data in the near future.

For the above reasons, the main purpose of this research is to give an insight to the Audit Board that data matching system in e-Audit is one of the potential threats to privacy, if this system is not managed in a wise manner and specifically due to the absence of a clear mechanism. In addition, the expectation of the author is this research can motivate the Indonesian government to design a complete and comprehensive legal framework concerning to privacy and data protection in Indonesia. As part of a global community, Indonesia must adapt according to international standards in order to arrange various activities with other countries. One of the most crucial activities involves economic growth through international trading. The European Union market is one potential market for Indonesia. However, the European Union is very strict on matters relating to privacy and the protection of personal data, specifically when data on its citizens is transferred among countries (see below, section 4.3). For this reason, Indonesia must prepare a complete and comprehensive legal framework in the field of privacy and data protection.

First of all, this research will focus on exercising how the data matching system in e-Audit may threaten privacy. This examination aims to determine whether the existing Indonesian legislations adequately respond to the threats to privacy in connection to the data matching system in e-Audit. Furthermore, this research will be more valuable if the examination results are compared with the current EU regulatory framework. Comparing the examination results to the EU legal framework is conducted in order to accommodate the possible insufficiencies within the Indonesian legal framework in relation to the threats to privacy because of the data matching system in e-Audit.

In Chapter 4 (particularly section 4.2.1) I shall discuss further the reasons why the examination results in this research should be compared with the current EU regulatory framework and why Indonesia should adopt some aspects of the current data protection directive (Directive 95/46/EC), even though Indonesia and the EU have different concepts of privacy.

---

30 General financial transactions in this context such as comparing financial transactions in the accounting system of institutions (SAI) and financial transactions in the general state treasurer (BUN). <http://www.scribd.com/doc/96399632/Perkembangan-E-Audit-6-Februari-2012-1>. As cited on July, 18, 2012.

1.2 Research Questions

Based on those problems, the following main research question is formulated into this thesis:

“Is the Indonesian legal framework sufficient to respond to the threats to privacy as a result of the data matching system in the context of e-Audit?”

Below are four sub-questions identified to answer the main research question. These sub-questions will be separately answered within the chapters of this thesis:

1. How does the data matching system work in the context of e-Audit?
2. How might the data matching system in e-Audit threaten privacy?
3. How far do the existing Indonesian regulations adequately respond to the threats to privacy in consequence of the data matching system in e-Audit?
4. What lesson can be learned from the EU regulatory framework concerning the threats to privacy in relation to the data matching system in e-Audit?

1.3 Methodology and Structure

To answer the main research question and the sub-questions, this research is firstly based on a literature study to get a better understanding with regard to the data matching system in the context of e-Audit. It is required to describe and to interpret both the Indonesian and the EU regulatory framework, in order to obtain a strong analysis. In addition, describing and interpreting both different legal systems will familiarize the reader with these regulations.

As a result, policy papers and legislations are used as the primary sources, whereas scholarly literature acquired mainly from online databases containing journals and e-books, are considered as secondary sources. These documents are chosen because they can provide a clear picture in the field of inquiry, so that they can support and sharpen the legal analysis. Moreover, expert opinions, working group documents, conference notes and documentation issued from authoritative bodies, such as ASOSAI, EUROSAI, and INTOSAI have been used to broaden the view on the subject matter.

---

32 ASOSAI is one of the regional (Asia) groups of the International Organization of Supreme Audit Institutions <http://www.asosai.org/>. As cited on August 28, 2012.
33 EUROSAI one of the regional (Europe) groups of the International Organization of Supreme Audit Institutions <http://www.eurosai.org/>. As cited on August 28, 2012.
Since some parts of this research discuss the data matching system in e-Audit, understanding technical terminologies in the field of both auditing and information technology is a difficulty in conducting this research. Therefore, these terminologies have been discussed with an officer\(^{35}\) from the Bureau of Information Technology in order to gain a better understanding.

In the above view, the main research question is defined into more detailed sub questions which are dealt in the different chapters of this thesis.

The second chapter highlights the data matching system in e-audit. First of all, the definition of e-Audit will be provided, and the table that explains the period of the development of e-Audit will be presented, as well. Then, I will thoroughly discuss the business process and the components that support e-Audit. Furthermore, this chapter will inform the reader more about the data matching system in e-Audit, including the input, the process and the output of the data matching. In addition, a picture will also be presented, so it is easier for readers to grasp the way how the data matching system works in e-audit. It is important to note that most of the descriptions in this chapter are based on policy documents of the Audit Board, such as the grand design of e-Audit, the speech of the chairman of the Audit Board, and the implementation report of e-Audit in 2011. Its objective is to give a clear illustration concerning the data matching system in e-Audit.

The third chapter aims to discuss the concept of privacy and its threats that might be arise because of the data matching system in e-Audit. First of all, the explanation related to the basic concept of privacy and its threats will be described. Besides, to answer the sub-question of this part, using the “IPO model”\(^{36}\) approach will be easier to identify the threats to privacy in each element of the data matching system.

Furthermore, by using the correlations between the issues in chapter two and three of this research, the fourth chapter will provide an analysis whether the threats to privacy because of the data matching system in the context of e-Audit has been accommodated by the Indonesian regulatory framework. A European case will be presented in this chapter, in order to give an insight that although the government agencies have legitimate grounds in processing personal data, but they also have limitations in accessing personal data. The EU regulatory framework will be discussed to give a comparative insight. The United Nations e-government survey of 2012\(^{37}\) reveals that most of the world e-government development leaders are the member states of the EU.\(^{38}\) Thus, comparing the Indonesian legal framework

\(^{35}\)Novis Pramantyabudi, The Head of Division of The Development of Computer Applications in The Bureau of Information Technology, The Audit Board of The Republic of Indonesia.


\(^{38}\)Member states of the EU that include the top 20 countries in world e-government development leaders 2012 are: The Netherlands, United Kingdom, Denmark, France, Sweden, Finland, Germany, Luxembourg, and Estonia. <Ibid>.
to the EU legislative framework will provide valuable insights to fill the gap between the rapid development of information technology in Indonesia and possible insufficiencies within the Indonesian regulatory framework.

As the last part of this thesis, chapter five will provide answers to the sub-research questions of this thesis. Then, an integrated conclusion will answer the main research question. The final chapter also includes recommendations in the interest of solving the remaining problems.
CHAPTER 2– Data Matching System in the Context of e-Audit

2.1 Introduction

In this chapter, I will describe how the data matching system works in the context of e-Audit. In order to provide a clear description, it is necessary to outline e-Audit at the beginning of this chapter, considering the data matching system is operated within e-Audit. Further, as stated before in the subchapter of the data matching system, the input, process, and output approaches will be presented in consideration of facilitating to describe the data matching system into more detail.

2.2 e-Audit

Before we discuss e-Audit into more detail, explaining the definition of e-Audit is essential in order to get a better understanding about the e-Audit. The definition of e-Audit, as laid down in the Grand Design of e-Audit, is:

“a system that builds synergy between the Audit Board’s information system (e-BPK) and the auditees’ information system (e-auditees) through an online communication between e-BPK and e-auditees, besides this system also develops a data center of management and accountability of public finances in the Audit Board.”

Based on the above definition, it should be noticed that there are no differences related to the cycle of an audit process, between e-Audit and the traditional audit. In this case, e-Audit is solely as an audit tool to simplify the audit process, specifically in analysing the audit data. As stated, “the Audit Board’s guideline of management audit 2008,” the audit cycle of an audit process starts with “organization of audit work plan, audit planning, implementation of audit, reporting of audit results, monitoring on the follow-up of audit results, and evaluation of audit.” The differences between them merely concern the utilization of technologies with respect to the efficiencies (time, human resources, and budgeting) and the effectivity, in view of the quality of the audit data.

According to Hadi Poernomo, there are some reasons that encourage the Audit Board to implement the e-Audit strategy. The first relates to transparency issues. The Indonesian government is accountable for the public funds it spends, which means that government agencies in Indonesia must be audited in order to monitor their accountability. The Audit Board was therefore mandated by the 1945 Constitution of Indonesia to audit state finance

---

40 Panduan Manajemen Pemeriksaan 2008 (The Audit Board’s guideline of management audit 2008) is one of audit guidelines in the Audit Board that are used as an operational basis, in performing its constitutional mandate.
41 Indonesia, BPK RI, *Panduan Manajemen Pemeriksaan* (Jakarta: 2008)68.
42 BPK RI, *Grand Desain e-Audit Menuju BPK Sinergi* 4-5.
43 Hadi Poernomo is the chairman of The Audit Board of The Republic of Indonesia (2009-2014).
44 Poernomo, 1.
management and accountability. In connection with transparency issues, the Audit Board is under an obligation to publish its audit reports for the public and to submit the audit reports to the House of Representatives as a proof of the fact that public funds have been spent timely, accurately and effectively. In addition, as I mentioned earlier, the high level of corruption in Indonesia has resulted in the Audit Board implementing e-Audit, in order to make the auditing process even more efficient and effective. What’s more, e-Audit will widen the scope of audits (the content and the number of entities that can be audited) in order to prevent and mitigate the level of corruption in Indonesia.

The second reason to implement e-Audit is the unbalanced condition regarding the number of the auditors (2,700), compared to the number of the audited entities (more than 2,000). Moreover, based on the existing regulation, the Audit Board has to submit the audit reports of financial statements to The House of Representatives and to The House of Regional Representatives, as well as to The Regional Representative Councils no later than two months after receiving unaudited financial statements from the government. In the same time, it could be that the Audit Board has to meet the time requirement from the Parliament to submit certain audit reports to the Parliament, as well.

As a proof of the Audit Board’s concern to “improve the function of audit management,” the Audit Board has inserted the e-Audit strategy into its “strategic plan” document (2011-2015). It means that the Audit Board will develop e-Audit for five years (2011-2015). Detailed activities of e-Audit in the Audit Board are described in the table below:

---

45 Law Number 15 Year 2004 article 17 (1-6) put an obligation to the Audit Board to submit its audit reports to The House of Representatives, The Regional Representative Councils, The House of Regional Representatives, Governors, Mayors and Regents <my own translation>.
46 Poernomo., 3.
47 Ibid., 2-3.
49 Poernomo., 3.
51 The Audit Board’s strategic plan is a document consists of strategies and policies that will be taken within every five years.
Creating synergy among thousands of audited entities is a “challenging homework” for the Audit Board. To simplify the homework, since 2011, the Audit Board has initiated to invite the audited entities to sign a Memorandum of Understanding between the Audit Board and the audited entities. The Memorandum of Understanding regulates the mechanisms on how to access the data, including a requirement for the audited entities to guarantee that they provide a complete and accurate data to the Audit Board.

Until the 13th of July 2012, there are 623 audited entities (Ministry: 34 entities; Institution: 48 entities; State-owned enterprise: 143 entities, and Local Government: 398 entities) that have signed the Memorandum of Understanding.

In 2011, The Audit Board conducted a pilot in order to measure the implementation of e-Audit. The pilot was conducted under 17 audited entities, and focused on the interim audit (as a preliminary audit before conducting the financial audit). In addition, the pilot of e-

53The analysis legal aspect is focused to analyse on the legitimate grounds in performing e-Audit.
54The guidelines consist of: (1) the guideline of management of e-Audit documentation, (2) the guideline of data structure, (3) the guideline of data security, (4) SOP of data acquisition, (5) SOP of the utilization of e-Audit data, (6) SOP to restore data, (7) SOP of data retention and data deletion, (8) SOP in utilizing the command center, and (9) the guideline of e-Audit Piloting. <Indonesia, BPK RI, Laporan implementasi e-Audit 2011 (Jakarta:2012) 15-17>.
55Randomly checked to three MoU: (1) the local government, (2) the state-owned enterprises, and (3) the institution.
Audit project was continued in 2012 as a “financial audit”. It is applied to the same 17 entities and other audited entities that already have structured data. With regard to the business process of e-Audit, the figure below describes that e-Audit allows to provide features that are possible to accommodate activities associated with data consolidation processes, audit correspondences, and the utilization of data from the “link and match” process online and in realtime. For more details, see the figure below:


Notes: - LK is a financial statement;
- DB is database;
- LHP is the audit report,
- IMG is image;
- AK is agent consolidator; and
- PIC is personal internet communicator.

---

58 It is should be noted that not all data from the audited entities are transferred to the Audit Board in realtime. It depends on the types of the data. For instance, in Directorate General of taxation, it is impossible to send their data in realtime, considering they have to reconcile their financial transactions before the data are transferred to the Audit Board. The Audit Board through the MoU does not have any authority to insist the audited entities to transfer their data to the Audit Board in realtime. <BPK RI, Grand Desain e-Audit Menuju BPK Sinergi 12>.
Based on the picture above, it can be noticed that there are several components involved in the implementation of e-Audit.  

1. Component that provides information and correspondence

1.1 e-Audit portal

An e-Audit portal is built to collect information, which is located in different places. An e-Audit portal is useful for both the Audit Board and other external parties to access information and applications based on the web. An e-Audit portal gives benefits to the Audit Board in reducing the administrative works, e.g. entities can submit the follow-up of audit results online and are able to track the follow-up of their audit results and monitor the indemnification of public loss cases through one gate.

Remembering audit data is confidential, besides implementing approval, authorization, and authentication mechanisms, to guarantee that one entity can not access other entities’ data, the Audit Board designs e-Audit Portal by “mutual exclusion data exchange.” It means the audit data from various entities that have been collected will be separated. Therefore, the entities that access their own data by using similar infrastructure with other entities, only can notice and communicate to e-BPK with their own data.

1.2 Command Center

Command center is “A system that functions as a “bridge” for auditors in accessing BPK’s data center.” In the command center, there is “end user computing” as a system to develop automation functions and to make reports on the basis of computer assisted audits. The command center is provided in the headquarters and 33 regional offices of the Audit Board. Moreover, the command center can be a special room equipped by scanners, printers, and several workstations or computers which connects to e-Audit and can be utilized by the auditors.

2. BPK’s Data Center

BPK’s Data center is “a center for collecting and managing structured or unstructured “raw data” and “processed data” that come from entities.” These entities’ data structures

---

59 BPK RI, Grand Desain e-Audit Menuju BPK Sinergi 17-20.
60 Ibid.,17.
61 Ibid.,17-18.
62 Ibid.,18 <my own translation>.
64 BPK RI, Laporan Implementasi e-Audit 2011 13.
65 Ibid.
66 Raw data is a term for data collected from a source that have not been subjected to processing or any other manipulation. <http://en.wikipedia.org/wiki/Raw_data>. As cited on July 15, 2012.
are classified based on the level of similarities and classified into general data, specific data, and unique data.\textsuperscript{69}

The process of collecting data from entities can be done by various means:\textsuperscript{70} (1) data exchanges through a “point to point data communication network” among the Audit Board and the entities; (2) entities that upload the data through an e-Audit portal; and (3) manually. “Manually” means the auditors access the audit data during the auditing process in the audited entities’ offices, or the audited entities give or send the audit data directly to the Audit Board. Then, using “document management”, nonelectronic audit data are processed into electronic data.

A mapping of data structures will be applied to deal with the differences of the data structures among the audited entities. Then, the data structures that have been mapped are ready for the matching process in BPK’s data center.

I mentioned before that the Audit Board has legitimate grounds for processing personal data. The Audit Board’s authority to process personal data by implementing the matching system will improve the quality of the audit data through extensification and intensification mechanisms. An extensification mechanism means the matching system that is supported by the components in BPK’s data center allows the Audit Board to obtain more detailed data to support an audit report. In the meantime, the intensification mechanism ensures that the Audit Board obtains appropriate and valid auditing data.\textsuperscript{71}

As a result, the data matching process in e-Audit allows the Audit Board to access the audit data not only during the implementation of an audit. During the audit planning phase, the data matching will assist the Audit Board to measure the level of the need of an entity to be audited by the Audit Board. In addition, during the audit processes, auditors can apply e-Audit for substantive\textsuperscript{72} and analytical\textsuperscript{73} procedures on the existing transactions.

\textsuperscript{67}Processed data is data that have been processed or manipulated. <wiki.answers.com/Q/What_are_the_stages_of_data_processing>. As cited on July 18, 2012. In the context of e-Audit, most of the audit data that are collected are “processed data”, considering the data have been used for more than one purpose (re-using of personal data).

\textsuperscript{68}BPK RI, \textit{Grand Desain e-Audit Menuju BPK Sinergi} 19 <my own translation>.

\textsuperscript{69}BPK RI, \textit{Laporan Implementasi e-Audit 2011} 20.

\textsuperscript{70}Ibid.

\textsuperscript{71}Ibid.,2.

\textsuperscript{72}Substantive audit procedure is a direct test of a financial statement balance designed to detect material misstatements at the assertion level <http://www.ais-cpa.com/glosa.html>. As cited on May 3, 2012.

\textsuperscript{73}Analytical procedure is a comparison of financial statement amounts with an auditor’s expectation. An example is to compare actual interest expense for the year (a financial statement amount) with an estimate of what that interest expense should be. The estimate can be found by multiplying a reasonable interest rate times the average balance of interest bearing debt outstanding during the year (the auditor’s expectation). If actual interest expense differs significantly from the expectation, the auditor explains the difference in audit documentation <http://www.ais-cpa.com/glosa.html>. As cited on March 3, 2012.
A BPK’s data center is built by a design that supports the implementation of an “intelligent business model” which is integrated with the master of consolidator agent. Some subcomponents of BPK’s data center are:

2.1 BPK’s Data Service

BPK’s data service is “a component to run automatic features of business processes that relates to an audit process in the Audit Board based on the instructions that are given.” It is used to process the electronic data in BPK’s data center, and it also functions as a “bridge” between applications and database.

2.2 Data Warehouse

This component consists of a database, designed for structured functions of data reporting and presentation of the data analysis. Those three components support a decision making process. A data warehouse in an e-Audit is built by classifying the data based on the entities’ groups, such as a group of the ministry, state-owned enterprise, the institution, the local government and the central bank.

2.3 Data Quality Management

Data quality management consists of features that enable to standardize data from some sources. These features are used to identify duplications with various degrees of similarities, and to give suggestions or data choices that have been regarded as the most accurate data based on specified criteria. It also provides a temporary storage for the inconsistent data before being standardized.

3. Consolidator Agent and Master of Consolidator Agent

Consolidator Agent and Master of Consolidator Agent are “a pair of application which function as ETL (Extract, Transform, Load) from data sources in entities’ database to BPK’s data center.” These components function as an early warning system which gives an automatic notification when the ETL process on consolidation of entities’ data occurred.

---

75 BPK RI, Grand Desain e-Audit Menuju BPK Sinergi, 19.
76 Ibid.
77 Ibid.
78 Ibid.
79 Ibid.
80 Ibid.
81 Ibid., 20.
82 Ibid.
4. Document Management

This component is a system which processes nonelectronic audit documents into electronic documents and manages electronic audit documents including electronic audit worksheets. Document management comprises storage, numbering, indexing, publication, browsing, searching and filing of electronic documents. 83

Shortly, based on the above picture and explanations, the business process of e-Audit can be described from the audited entities’ databases that are equipped by the consolidator agent that has the abilities for the ETL process. It means that before the data is sent to BPK’s data center, the agent consolidator will “extract, transform, compress, and encrypt” 84 the data. Next, the data will be sent to BPK’s data center through the Internet (public network) as their communication network. Like the audited entities’ databases, BPK’s data center is also equipped by the master of consolidator agent.

For the reason of security issues, the Audit Board uses HTTPS “(HTTP over SSL or HTTP Secure).” 85 The master of consolidator agent will “decrypt, uncompress, and load” 86 the data to BPK’s data center. Then, in BPK’s data center, the data will be processed by the components in BPK’s data center (BPK’s data service, data warehouse, and data quality management), particularly to standardize the format of the data before they are ready for the matching process. In addition, the table concerning activities of the Audit Board during the implementation of e-Audit describes “data standardization” has a significant role in the matching process. Therefore, the Audit Board inserts “data standardization” as one of the activities that have been focused during the development of e-Audit.

---

83 Ibid.
84 Indonesia, BPK RI, Konfigurasi dan Mekanisme Aplikasi Konsolidasi Data 1. Encryption is “the conversion of data into a form, called a ciphertext (encrypted text) <http://searchsecurity.techtarget.com/definition/encryption>. As cited on July 15, 2012. Data extraction is the act or process of retrieving data out of (usually unstructure poorly structured) data sources for further data processing or data storage (data migration) <http://en.wikipedia.org/wiki/Data_extraction>. As cited on July 15, 2012. Data transformation converts a set of data values from the data format of a source data system into the data format of a destination data system <http://en.wikipedia.org/wiki/Data_transformation>. As cited on July 15, 2012. Data compression is a process of reducing the amount of data needed for storage or transmission of a given piece of information (text, graphics, video, sound, etc.), typically by use of encoding techniques <http://encyclopedia2.thefreedictionary.com/data+compression>. As cited on July 12, 2012.
For the data that are collected manually, document management will process the nonelectronic data into the electronic data. After this phase, the audit data are ready to be used by the auditors through the command center for an audit purpose.

Meanwhile, e-Audit portal functions as a browsing tool, in order to know the audit status and human resources data, recording the follow-up on the Audit Board’s recommendations, completion of recommendations, Information pertaining to the indemnification of public loss cases, and uploading the electronic data with contents and formats that have been agreed upon.

It is important to bear in mind that in every stage of the development of e-Audit, the Audit Board has designated quality controls to guarantee that the process of e-Audit development runs well. The quality controls are appointed from internal departments of the Audit Board: (1) The Bureau of Information Technology; (2) Inspectorate General; and (3) Directorate for Planning, Evaluation, Development, Education, and Training.

It is uncontested, that the existence of e-Audit is useful not only for the Audit Board, but also for the entities. Therefore, as stated by Hadi Poernomo “by the synergy and the e-Audit, the Audit Board would like to shift a perspective of the audit as a burden into a need.” Hence, the Audit Board urges all the audited entities to join this data link and match project. Thus, the vision of the implementation of e-Audit is: “an audit transformation from a burden and obligation into an organisational requirement.”

2.3 Data matching system

The development of information technology enables people to modify, manipulate and match various types of data. With regard to the data matching system in e-Audit, understanding the definition of ‘data matching’ will build a clear concept in connection with its system. In general terms, ‘data matching’ means comparing the data that have relations with one another. Unfortunately, until now, data matching has not been defined officially in computer dictionaries, even though data matching has existed since the United States conducted the “project match” in 1979.

---

87 According to Law 15 Year 2004 article 1 (12), a recommendation of an audit report is an auditors’ recommendation based on their audit results and addressed to a person and/or an authoritative body to carry out an action or improvement <my own translation>.
89 Ibid., 22.
90 Poernomo, 4.
91 BPK RI, Grand Desain e-Audit Menuju BPK Sinergi 3 <my own translation>.
93 “Project Match” was administered by Department of Health, Education, and Welfare. This program is a program seeks to expose law breakers by matching state welfare rolls with lists of Federal employees. Therefore, computers are used to effect a complicated series of data exchange between the Federal and State
Steinbock (2005), states that data matching is a part of data mining. Further, Minow and Cate (2008) define data mining as “a wide spectrum of data-based activities ranging from ‘subject-based’ searches for information on specified individuals to ‘pattern-based’ searches for unusual or predetermined patterns of activities or relationships.” The other terms of “data matching” (as cited in Steinbock, 2005, p.10) are “computer matching” (Cohen,1986) and “subject-based inquiry” (Clarke, 1995). Steinbock (2005) defines “data matching” as “the computerized comparison of two or more systems of records.” Meanwhile, GAO (1986) uses the term of computer matching in order “to compare two or more files containing information on people or organizations of interest to the government.”

Further, the following definitions provide a clear interpretation of data matching and data mining. Data matching is “the large scale comparison of records or files that are collected or held for different purposes, with a view to identifying matters of interest.” Meanwhile, data mining has been defined as “a set of automated techniques used to extract buried or previously unknown pieces of information from large databases.”

In implementing e-Audit, the term “data matching”, which the Audit Board uses in e-Audit, is used to describe the interconnection of the audit data in e-Audit. However, the techniques used are quite similar to data mining, i.e., clustering that is used “to identify groups of similar cases” and classification, meaning “the ordering of data into groups or classes on the basis of their similarity.” Moreover, the Audit Board performs data matching based on analytical procedures of the auditors in order to process data through an automation process. Nonetheless, it should be noted that the scope of data matching in implementing e-Audit is not as large as data mining for law enforcement purposes. For instance: using the assistance of the intelligence agencies.

Considering the absence of an official definition of data matching, it is useful to recognize the characteristics of data matching: “(1) correlation of two or more databases; (2)
significant number of matched data; (3) automated matching algorithm; and (4) result of administrative actions.\textsuperscript{103}

In general, people merely know that data matching is applied in the area of law enforcement. Basically, the purposes of data matching are various, such as: detection and deterrence of fraud, verification, identification of corruption, and for research purposes.\textsuperscript{104}

In connection to the Audit Board as an audit institution, the main purpose of conducting data matching is to prevent and to detect any types of fraud and abuse in the area of public finance management.

Data matching is a system, so it indicates that there is more than one party involved in the data matching system. In the data matching system in e-Audit, the parties that participate in the system are classified into two parties:

1. The audited entities

There are more than 2,000 audited entities that provide data for the matching process. There is not any limitation regarding to the amount and the forms or media of the data that will be provided. Based on Law Number 15 Year 2004 article 10 (a) and (b) and Law Number 15 Year 2006 article 9 (1) point ‘b’ and ‘d’, and article 9 (2), the Audit Board has authority to ask and to access any types of data from the audited entities and third parties, as long as those data have relations to the state finance management.

2. The Audit Board

The Audit Board is the party that both runs the matching process in its data center and utilizes the output of the matching process.

Previously at the beginning of this chapter, I have already mentioned that to facilitate describing of data matching into more detail, I prefer to mention data matching by a system. In general, a system consists of input, process and output. Therefore, by using the “IPO model”\textsuperscript{105} approach, business process of the data matching system in the context of e-Audit consists of :

1. Input

Input is “the information, ideas, and resources used in creating a program.”\textsuperscript{106} There are various resources that could be input in the data matching system, such as software, hardware, and all of the data from the audited entities and the third parties that have relations to the state finance management.

\textsuperscript{103}Papakonstantinou, 46-48.
\textsuperscript{105}<http://en.wikipedia.org/wiki/IPO_Model>. As cited on July 14, 2012
\textsuperscript{106}Ibid.
The audited entities have different functions in the Indonesian governmental system. Therefore, each of them has different business processes and different data structures. Usually, the data from the audited entities have formats in: *.dbf (database), *.csv\textsuperscript{107}, *.mdb (Ms. Access) or other formats that have been agreed upon between the entities and the Audit Board.\textsuperscript{108} These various formats of the data, that have been selected by the audited entities based on request from the Audit Board are changed through the ETL process into *.mdf (Ms. SQL Server Database) format. This process is conducted by the consolidator agents that support the audited entities’ databases. Then, the data are ready to be sent to BPK’s data center.

2. Process

As mentioned above, the matching process is operated in BPK’s data center designed by an intelligent business model and supported by three subcomponents. In this part, I will describe the data matching process in e-Audit, and how the components in BPK’s data center participate to the matching process.

Firstly, data from the audited entities will be stored in the data warehouse as the database of the Audit Board. Then, data warehouse is built by the classifications on the data, based on the entities: the local government, the ministry, the institution, the state/local-owned enterprises, and the central bank. Considering that data standardization is the success key for the data matching process, data quality management will standardize the structures of the data from the audited entities. The standardization will be based on the degree of similarities from the data and the types of entities. Subsequently, BPK’s data service is used to process the electronic data from the data warehouse, based on the criteria or instructions that are given. In this phase, the matching algorithms\textsuperscript{109} will analyse the possibility of the interrelationships\textsuperscript{110} of the data from one entity to others.

The next step is that the algorithms will identify the “hit” as the data that meet the criteria from the given instructions and are selected by the matching process.\textsuperscript{111} According to Naps (1992), the algorithm itself means “an unambiguous sequence of clear instructions that will solve a given problem in a finite amount of time and then halt” (as cited in Steinbock, 2005, p.13).


\textsuperscript{108} BPK RI, Laporan Implementasi e-Audit 2011, 20.

\textsuperscript{109} Papakonstantinou, 43.

\textsuperscript{110} BPK RI, Grand Desain e-Audit Menuju BPK Sinergi, 5.

\textsuperscript{111} Office of The Information and Privacy Commissioner/Ontario, 37.
3. Output

Output is the “results of the processing that then exit the system.” Generally, the output of data matching could be organizational profiles and/or personal data profiles. However, details of the output will depend on the criteria that are applied during the matching process.

In the context of e-Audit, the output of the matching process will be used by the Audit Board in order to support the decision making processes on an audit process. These decision making processes will give contributions before, during, and after an audit process.

As an illustration, if the output of an investigative audit in a corruption case includes personal profiles, particularly ones related to financial transactions, these can help the auditors to analyze the financial transactions of suspects in order to indicate whether fraud has been committed, for instance, in order to trace whether public funds have been wrongly transferred to a suspect’s personal account. The suspect’s personal data are then subjected to further analysis in order to determine the fairness of the suspect’s financial transactions.

It can be concluded that the “IPO model” in the data matching system is developed by the integration of e-Audit components, the algorithms, and the intelligent business model that allow to improve the capabilities of the system. However, it should be underlined that the output of the system will depend on the input and the process of the system. It means, the output of the data matching system in the context of e-Audit relies on three factors: the quality of the data as the input, software, and hardware that support the components in BPK’s data center for the matching process.

The fact that the output of the data matching system will be used as support when formulating an audit report should be borne in mind, so it is important to explain the structure of an audit report and the degree to which Indonesian legislation limits public bodies from disclosing personal information to the public.

Basically, an audit report consists of several audit findings. Each of the audit findings comprises: (1) condition: consists of information based on facts; (2) criteria: conditions that are expected, based on existing regulations; (3) effect: explaining logically the effects that arise because of the differences between the condition and the criteria; (4) cause: explaining the evidence pertaining to factors

---

113 BPK RI, Panduan Manajemen Pemeriksaan 45.
that lead to differences between the condition and the criteria; and (5) recommendations.\textsuperscript{114}

In practice, the recommendations of an audit report have implications to: (1) administrative issues; (2) indemnification for public loss cases; and (3) legal proceedings for fraud that contains criminal elements.

As mentioned previously, the Audit Board has legitimate grounds to process audit data from both the audited entities and third parties. Therefore, the recommendations of an audit report are binding not only to the audited entities, but also to the third parties. Law Number 15 Year 2004, article 26 (2):

“Everyone who does not fulfil the obligation to follow up the recommendations of an audit report will be punished with a maximum of 1 year and 6 months imprisonment and/or a fine of Rp 500.000.000,00 (five hundred million rupiahs).”\textsuperscript{115}

With regard to the privacy issues, the Audit Board does not have any standard regulating how personal information in audit reports should be disclosed or shielded. The only limit imposed on public bodies regarding the disclosure of personal information in existing Indonesian legislation is laid down in article 17 (h), Law Number 14 Year 2008:\textsuperscript{116}

“Every public agency is obliged to provide access to obtain public information for every public information applicant, except Information that if disclosed and supplied to public information, applicant may reveal a personal secret, ie:

(1) the history and condition of a member of the family;

(2) the history, condition and care, physical medical treatment, and physic of an individual;

(3) the financial condition, assets, income and bank account of an individual;

(4) evaluation results of the capability of an individual; and/or

(5) personal notes of an individual pertaining to his/her formal education and non formal education activities.”

Nowadays, the Audit Board publishes audit reports for the public by: (1) publishing the summary of the audit reports every semester in each year on the Audit Board’s official site; (2) announcing the summary of certain audit report by means of a press release describing the audit findings on the Audit Board’s official site; and (3) parties that need a complete

\textsuperscript{114} See supra note 87.

\textsuperscript{115}<my own translation>.

version of an audit report can request one, as long as they meet the Audit Board’s requirements.\textsuperscript{117}

However, the 33 regional offices and 1 head office of the Audit Board have various ways of disclosing personal information in an audit report. Below are some models pertaining to the disclosure of personal information in an audit report from several websites:

1. The audit report on financial audit No. 23.C/LHP/XVIII.BDG/07/2011, on July 6, 2011. One of the audit findings stated that there was a fictive transaction for the procurement of printed materials. Page 9 of the audit report mentioned a suspect’s initials, “RNR”, as the officer of a budgeting division in local government in Indonesia. It also mentioned “RNR’s” personal account number: 0006957110100 with “BJB” bank.\textsuperscript{118}

2. The audit report on financial audit No. 90/R/XVIII.JATIM/05/2009, on May 31, 2009. One of the audit findings in the audit report referred to an indemnification in a public loss case because a public official in local government lost an official car. Page 69 of the audit report stated the initials, “Ir. SK ET”, naming him as an official in local government in Indonesia. He is under an obligation to compensate for the car and pay the indemnification by instalments. However, the audit report later referred to the complete name of “Ir. SK ET” as “Ir. Soewignjo Koes ET” and revealed that the payroll of “Ir. SK. ET” is insufficient to be able to pay the instalments.\textsuperscript{119}

In connection with the corruption issue in Indonesia, article 14 (1) Law Number 15 Year 2004, prescribes that the Audit Board reports to law enforcement agencies if there are indications of criminal elements “during” an audit process. The aim of the article is to accelerate the process of eradicating corruption in Indonesia. As a result, since 2006 the Audit Board has signed several memoranda of understanding with related parties in order to mitigate the level of corruption in Indonesia.\textsuperscript{120} Furthermore, these memoranda regulate that, for reasons of law enforcement in Indonesia, the Audit Board is allowed to hand over audit reports and “audit data”\textsuperscript{121} to law enforcement agencies.

\textsuperscript{117}In order to prevent the abuse of the audit reports, the Audit Board prescribes parties to fill out a form regarding their personal data and the purpose of the utilization of the audit reports.


\textsuperscript{120}The memorandum of understanding between the Audit Board and : (1) The Indonesian Corruption Eradication Commission in 2006; (2) The Indonesian Attorney General in 2007; and (3) The Indonesian Police in 2008.

\textsuperscript{121}Audit data in this context is not the audit report, but the data that support in formulating an audit report (the worksheets).
2.4 Conclusion

As explained previously, the initiative of the Audit Board to accelerate good governance in Indonesia is performed by utilizing the development of information technology through e-Audit. The implementation of e-Audit facilitates connection between the Audit Board’s information system (e-BPK) and the auditees’ information system (e-Auditees) through online communication.

The components in e-Audit (command center, e-Audit portal, BPK’s data center, consolidator agent and master of consolidator agent, and document management) facilitate the provision of different features for audit purposes.

One of the features provided by the e-Audit is the data matching process that assists the auditors in analysing the audit data. However, the matching process does not stand alone: it needs the existence of input in order to generate results. In fact, “data matching” should be regarded as a matching system rather than a process.

In order to obtain a clear and comprehensive description pertaining to data matching, the “IPO model” approach is applied to the data matching system in e-Audit.

This starts with the input phase that involves the existence of the consolidator agent in the audited entities’ databases. The consolidator agent performs the ETL process in order to deal with the issues concerning different formats and structures of the audited entities data. The second phase is matching process that is operated in BPK’s data center as one of the components in e-Audit. BPK’s data center has three elements that participate in the matching process. They are Data warehouse that functions as the Audit Board’s database that stores all data from the audited entities, Data quality management that standardizes the audited entities’ data, and BPK’s data service that has an essential role in the matching process through its matching algorithms. The last phase is the output that constitutes organizational profiles and /or personal data profiles. Both of them will give a contribution to support the decision making processes “before, during, and after” an audit process.

The main objective of the matching system is to correlate the audit data that are interconnected. Consequently, the application of the matching system in e-Audit generates not only complete, but also detailed audit data.

Nevertheless, managing myriad audit data through the automation process, particularly personal data, is not a simple task for the Audit Board, considering the nature of personal data which differs from public data. Though the integration of e-Audit components, the algorithms, and the intelligent business model may
improve the capabilities of the matching system, it may also form a threat to the privacy of the data owners.
CHAPTER 3– The Threats to Privacy

3.1 Introduction

As previously explained, the matching system in e-Audit has more significant involvement in analysing the audit data than the “link” process. Therefore, this chapter will answer how the data matching system might threaten privacy.

First of all, in order to obtain a comprehensive description of the threats to privacy, I will describe the concept of privacy and the threats to privacy. Furthermore, to determine the threats, the “IPO model approach” will be applied to identify every element in the data matching system.

Although the data matching system makes it possible to create both personal and organizational profiles, my research will be focused on the discussion of personal profiles since public bodies have a tendency to access personal data excessively.122

3.2 The concept of privacy and threats to privacy

Privacy is one of a human being’s fundamental rights, like the right to liberty and the right to freedom.123 Generally, the protection of privacy has been guaranteed in article 12 of the Universal Declaration of Human Rights.124 People have also become familiar with the concept of privacy through both “The International Covenant on Civil and Political Rights”125 and regional and international treaties.126 The 1945 Constitution of Indonesia does not adhere to the principles described in the Universal Declaration of Human Rights, but it shares some similar principles with the declaration, including humanitarian principles.127 I will further discuss this issue in chapter 4.

The existence of privacy as an “abstract humanistic concept”128 must be protected, considering privacy consists of values such as dignity, respect, and integrity of human

122Office of The Information and Privacy Commissioner/Ontario, 36.
124Article 12:“No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.”< Ibid>.
beings. Additionally, in a democratic society, privacy is required as a reflection of individuals’ autonomy.\textsuperscript{129}

The Latin term for privacy means “separated from the rest.”\textsuperscript{130} However, since privacy is an abstract concept, it is difficult to define privacy in a way that can be applied universally. Moreover, how one country conceptualises the idea of privacy may be different from other countries. The diversity of social and cultural backgrounds leads to differences in their concepts of privacy.\textsuperscript{131}

Experts and scholars hold various opinions about the definition of privacy. Some of them define privacy as: (1) “the right to be left alone” (Warren & Brandeis: 1890); (2) “informational self-determination” (Westin: 1967); and (3) “the freedom from unreasonable constraints on the construction of one’s own identity” (Agre & Rotenberg: 2001).\textsuperscript{132} Those definitions indicate that there is a shift concerning the concept of privacy, from “seclusion”, changing into “self-determination” and ending with “identity building.” Hence, according to those definitions, Hildebrandt (2006) claims the “core of privacy is identity”.\textsuperscript{133}

Further, Banisar (2001) divides privacy into “information privacy, bodily privacy, privacy of communications, and territorial privacy.”\textsuperscript{134} This classification describes the coverage of the invasion of technologies into our private areas. However, it seems that this classification will also eventually lead to “identity”.\textsuperscript{135}

Banisar’s classification explains that:\textsuperscript{136} (1) information privacy is about how to protect personal information, for instance, medical records; (2) bodily privacy refers to the physical protection of a person from invasive procedures, for instance, fingerprinting; (3) communication privacy refers to the protection of our telephone conversations and electronic mail, for instance from interception; and (4) territorial privacy means protection in our private space, for instance, safeguarding our homes from being monitored by satellite for the sake of public security. It is important to underline that a medical record provides information on a person’s diseases; fingerprints describe a person’s unique identity; a telephone conversation and electronic mail provide insight into a person’s intelligence and their character, and the condition of a person’s home provides insight into their economic

\textsuperscript{129}Foran, 1999.
\textsuperscript{131}Iachello and Abowd, 91.
\textsuperscript{133}Hildebrandt, Privacy and Identity 7.
\textsuperscript{135}According to James D. Fears: “Identity” in its present incarnation reflects and evokes the idea that social categories are bound up with the bases of an individual’s self-respect.” James D. Fears,“What Is Identity (As We Now Use The Word)?”, 1999: 2. \textlangle \url{http://www.stanford.edu/~jfearon/papers/iden1v2.pdf} \textrangle . As cited on July 20, 2012.
\textsuperscript{136}\textlangle \url{http://gilc.org/privacy/survey/intro.html} \textrangle . As cited on August 28, 2012.
status. All these elements can affect the construction of people’s identities. Therefore, in this research I prefer to use the term “privacy” in the sense of Agre’s and Rotenberg’s definition, without making a further distinction between the various dimensions of privacy, as all of these have some relation to personal information and identity.

As stated above, privacy relates to personal information and its identification. Cavoukian and Chibba (2009) formulate that personal information includes “biographical, biological, genealogical, historical, transactional, locational, relational, computational, vocational, or reputational” aspects. Their classification implies that the scope of personal information seems to be limited to that definition. For instance, how about individual behaviour? I believe that individual behaviour does not merely relate to genealogical factors because our environment significantly contributes to influencing our behaviours. In other words, based on my opinion, Cavoukian and Chibba’s classification is inadequate for accommodating the concept of personal information. Therefore, Hildebrandt (2012) reformulates the definition concerning identity through a simple statement, but it has more extensive sense. She claims that identity does not merely relate to our ID, but it represents all information that is related to ourselves. Consequently, since personal information is the reflection of identity, we can conclude that privacy is the individual’s right that gives authority to us, as the only party entitled to control our personal information.

I re-emphasize Greenleaf’s analogy (2008) from Chapter 1 that compares personal information with copyright. Both of them have a bundle of rights and copyright that related to specific rights (adaptation, reproduction, etc). Meanwhile, in personal data, individuals have the right to access, limited collection, security, and so forth. In intellectual property rights, the holders of rights can transfer their rights to third parties. Conversely, in personal information, the individuals “will maintain their rights as to processing of their data”, even though they have given their consent to other parties’ in processing their data.

---


140 Foran, 1999.

141 Greenleaf, 11.

142 Ibid.


144 Ibid.
Thus, in my opinion, the scope of the term “control” in connection to privacy is basically the rights of individuals: (1) to determine which parties can access their personal information; (2) to control mechanisms for collecting, processing, and storing the information; (3) to determine readiness to disclose their personal information; and (4) to define or judge their personal information.

Previously, I stated that there has been a shift concerning the concept of privacy, triggered by the development of information and technology. Additionally, several characteristics of the internet (“global, instantaneous, intrinsically transborder, digital, and enables automated information processing”145) modify the ways in which technologies threaten the privacy sphere.

However, it cannot be denied that the development of information technologies does not merely have negative impacts. We can see how these kinds of technologies improve our lives with the efficiency and the effectiveness that they provide. Hence, in my view, the development of technologies is like two sides of a coin: on one side they play significant roles in improving our lives, while on the other side they threaten our lives, particularly in the area of privacy.

Nowadays, the utilization of personal data in government sectors and in business fields indicates that the number of privacy threats has increased.146 Nevertheless, at present, there is not any single official definition of the term “threats to privacy”. However, the word “threat” means “an expression of intention or an indication”.147 Thus, if I correlate it to that definition, “a threat to privacy” is an expression of intention or an indication of any type of invasion and interference in the area of privacy.

According to Foss (2008), there are various methods for determining threats to privacy. He classifies these threats into: “(1) hardware threats: monitoring devices (CCTV), hidden cameras, microphones, sensors, and etc.; (2) software threats: malicious programs, such as viruses, trojans, spyware, etc.; (3) web threats: tracking, data mining, data analysis, database leaks, phishing, cracking, and etc.”148

I believe that Foss simply classifies threats to privacy from a technical aspect. Therefore, to complete Foss’ classification, in my view the threats based on non-technical aspects are the government’s policies and the lack of a clear and comprehensive legal framework that relates to privacy.

---

A government’s policy is one example: the implementation of e-government by public bodies can be a threat to privacy because in recent years a lot of government programs have required personal information from their citizens. The authorities that are owned by the governments make it easy for them to collect, to store and to use citizens’ personal information. One of the threats that might emerge is “surveillance” of citizens by the government.\(^{149}\)

Therefore, as I stated in Chapter 1, the existence of clear and comprehensive regulations are required as powerful instruments, in order to respond the development of information technologies. Conversely, the lack or even the absence of a comprehensive legal regime that relates to privacy and data protection could be categorized as a threat to privacy.

### 3.3 Models of threats to privacy

It has been previously explained that a system will generally consist of input, process and output. In connection with threats to privacy caused by the data matching system in e-Audit, we will apply the “IPO model” approach to identify the threats from every element of the matching system:

1. Re-using personal data: a threat during the input phase

According to the discussion in Chapter 2, the input for the data matching system in e-Audit is the audited entities’ data. These data have different formats and structures since the audited entities have various business processes. Therefore, the matching process requires “data standardization”. My point is that data that are used as input in the data matching system may consist of the product of the re-used personal data.

In recent years, implementing e-government has become a new trend for accelerating good governance in Indonesia. The “interoperability”\(^{150}\) of the application of information systems among public bodies enables information sharing. As an example, the Directorate General of Taxation issues Tax Numbers (a kind of social-security number) based on data directly received from the taxpayers. However, to assure the level of asset ownership in Indonesia, the Directorate General of Taxation needs data from the Population and Civil Registration Office that pertains to information about the Indonesian population based on asset ownerships.\(^{151}\)

---


\(^{150}\) The definition of Interoperability as cited from IEEE Standard Computer Dictionary is “The ability of two or more systems or components to exchange information and to use the information that has been exchanged.” [http://arvantc40s.blogspot.nl/2012/02/interoperabilitas-data-dalam-e.html]. As cited on July 22, 2012.

In order to verify the truth regarding the amount of tax a person has already paid based on personal data that he has provided in relation to his asset ownership, the Directorate General of Taxation needs to compare the data with data from the Population and Civil Registration Office. This comparison is necessary in order to verify the numbers and types of assets that a person has. Furthermore, within the context of e-Audit, the Audit Board may request data from the Directorate General of Taxation for the purpose of an audit. For instance, in an investigative audit for a corruption case, the Audit Board will trace a lot of financial transactions relating to the suspect, including transactions relating to the suspect’s assets, in order to detect any unfairness in financial transactions and to verify asset ownership.

I believe that when a person gives his personal data to the Directorate General of Taxation, he does so only for taxation purposes. In view of this, the processing of personal data must be controlled, because it represents value that must be protected from unlawful processing. In fact, as the basis for the government’s programs for public interests, these personal data are actually processed frequently and for various purposes by public bodies. In addition, technological developments facilitate the expansion of processing, particularly the amount of personal data collected by government agencies. These circumstances make it difficult for data-owners to control their personal data, resulting in a threat to their privacy.

It is undeniable that the re-use of personal data through online communication between public bodies provides efficiency, both in time saved and, in particular, saving money the state spent on travel expenses. In addition, the information technologies do not only provide efficiency but also effectiveness in processing and transferring the data. Therefore, the utilization of information technologies may improve the performance of the government in front of the public.

With regard to the data matching system in e-Audit, we already noticed that its input not only consists of the original data from the audited entities (data that are produced by the entities), but also could be the product of the re-use of personal data. However, the speed of the flow in the re-use of personal data among public bodies may become a threat to privacy. Hence, even though not all public bodies in Indonesia have applied online communication, the existence of the interoperability allows the public bodies to exchange the collections of personal data that they own. Then, they utilize the data before finally the Audit Board processes the selected data as the input in the data matching system.\(^\text{152}\)

However, problems may arise because as I stated several times in my thesis, the automation process is very risky with respect to the quality of data. Moreover, the widespread exchange and transfer of personal data among public bodies, including the processing of personal data by the Audit Board as the input in the matching system, are performed without

\(^{152}\text{It is important to underline, considering the duty of the Audit Board is to audit state finances, in practice, the Audit Board only share the audit data for the law enforcement interests, with regard to the corruption case in state finances.}\)
informing individuals that their personal data are being processed for various purposes. These circumstances automatically ensure that individuals cannot enforce their rights to control the flow of their personal data.

We know that the re-use of personal data for the input in the data matching system is aimed at accelerating the realisation of good governance in Indonesia, but it should be balanced by enforcement of the individuals’ rights to control their personal data as a reflection of their dignity, respect and integrity. I believe that Indonesia is a democratic country that respects both the fundamental rights and the autonomy of individuals. We know that privacy is categorized as a derogable right, in which the enforcement of the right could be diminished under legitimate grounds. Therefore, in accessing personal data, the Audit Board does not need a specific consent from the individuals because the Audit Board already has legitimate grounds.

However, the processing of personal data by the Audit Board under legitimate grounds does not mean that individuals should not be allowed to realise anything about the processing of their data, including the information pertaining to the purpose of processing, the accuracy of their data and the storage location of their data in one database (in this case, BPK’s data centre). The speed of the flow of personal information among the audited entities and the absence of consent from individuals under the legitimate grounds to process personal data result in a situation where individuals cannot control the accuracy of their data through updating, challenging or adding some personal information based on current conditions.

One of the objectives in processing personal data through a reliable system is to provide audit data that can support the accuracy and validity of the data in the audit report. According to The Canadian Institute of Chartered Accountants, integrity is one of the requirements for creating reliable electronic audit data that can be used as “electronic audit evidence”, meaning that “the assurance that the information was validated and was not intentionally or accidentally altered or destroyed when it was created, processed, transmitted, maintained and/or achieved.”

155 See supra note 24.
156 The Canadian Institute of Chartered Accountants, Electronic Audit Evidence (Canada, 2003) 11. According to The Canadian Institute of Chartered Accountants, Electronic audit evidence is information created, transmitted, processed, recorded, and/or maintained electronically that supports the content of the audit report.
157 Ibid., 33.
Therefore, informing individuals about their processed data not only benefits the individuals by enforcing their rights, but also benefits the Audit Board by improving the quality of the data used as the input in the matching system. Even though one of the clauses in the “Memorandum of Understanding”\textsuperscript{158} stipulates that the audited entities have to guarantee the accuracy and completeness of the data used as input for the matching system, I believe, in practice, the audited entities cannot control the quality of all data considering the myriad of data and the speed of the flow of personal data.

Moreover, the matching system is a system, so the quality of the input will influence the output. As Schermer (2011) stated about the concept of data mining, “the success of a data mining exercise is dependent on the quality of the raw data being mined. If the data inaccurate, the results will also be inaccurate.”\textsuperscript{159} In addition, if individuals lose control of their personal data, it might not only threaten the quality of the input for the matching system but might also harm the individuals by causing embarrassment, lack of self confidence or even the loss of chances to improve their lives. Thus, Peter Hustinx from EDPS says: “The re-use of PSI containing personal data may bring significant benefits, but also entails great risks to the protection of personal data, due to the wide variety of data held by public sector bodies.”\textsuperscript{160}

2. Computer system: a threat for the process phase

Basically, a data matching process consists of two phases: (1) the pre-processing phase, and (2) the matching process phase. However, the pre-processing phase focuses on the data-cleaning process as I already explained when describing the ETL process. Therefore, the current discussion will focus on threats during the matching process phase.

As mentioned above in Chapter 2, during the matching process, algorithms play a significant role in analyzing possible data interrelationships between entities. In addition to identifying interrelationships, as part of mathematical procedures, algorithms can also be used to identify trends and hidden information.\textsuperscript{161}

Nevertheless, the abilities of the algorithms to identify the data that have interrelationships are supported by the computer system. Therefore, this “artificial intelligence’s”\textsuperscript{162} abilities may result in errors during the matching process, because of the hardware and software.\textsuperscript{163}

\textsuperscript{158}See supra text 55.


\textsuperscript{161}Hildebrandt, Profiling The European Citizen 65.

\textsuperscript{162}Artificial intelligence is the intelligence of machines and the branch of computer science that aims to create it. <http://en.wikipedia.org/wiki/Artificial_intelligence>. As cited on July 23, 2012.
A hardware error is “a malfunction in a hardware component in a computer system.”¹⁶⁴ For instance, an error in the “central processing unit”¹⁶⁵ will definitely influence the ability of algorithms to identify “hits” properly. A software error, however, refers to an “error resulting from a bad code in a program that is used, thereby resulting in an erroneous result.”¹⁶⁶

Data matching system in the context of e-Audit compares different types of data from thousands entities, but represent the same object.¹⁶⁷ Consequently, for the matching purpose, matching variables are applied.¹⁶⁸

Several problems may arise regarding the matching variables used. For instance, in the case of an investigative audit of a fictive official trip, the auditors apply the matching variables: name, family name, destination, day, date and purpose of the official trip. Duplicates may occur in a “data set”¹⁶⁹ involving a non-fictive trip. This means it is possible for one officer to make a fictive official trip, and the other officer, with similar identifiers, to make the real official trip. For instance: the first name of the officer who makes a real official trip is: “Christene”; family name: “Siregar”, and the destination of the official trip is “Bandung”. In the meantime, the first name of the officer who makes a fictive official trip is: “Kristene”; family name: “Siregar”, and the destination of this official trip is “Badung”.

However, because of the bad code or wrong criteria entered into the programme by the programmer, the algorithms grasp the hits of the officer who makes the real official trip. In this case, a lack of clarity in the instructions or criteria given to the algorithms and other details may lead to inaccuracies in output for the matching process.

According to Swarns (2004), this duplication effect in the matching process used to occur when airlines refused to allow such recognizable persons as Senator Edward Kennedy to board an aeroplane because his name on the passenger list resembled an alias used by a suspected terrorist.¹⁷⁰ As Theodore Roszak said, “every piece of software has some repertory of basic assumptions, values and limitations embedded within it.”¹⁷¹

¹⁶³Office of The Information and Privacy Commissioner/Ontario,41.
¹⁶⁵Central Processing Unit is “the brain” of the computer that can gives basic until complex instructions to the computer. <http://www.techterms.com/definition/cpu>. As cited on September 8, 2012.
¹⁶⁶<http://www.definitions.net/definition/software%20error>. As cited on September 8, 2012.
¹⁶⁸Ibid., 3.
¹⁷⁰Steinbock,60.
¹⁷¹Ibid.,61.
In a small company, a matching process usually only compares two simple fields and this is quite easy for the algorithms. However, e-Audit’s data matching process includes multiple and detailed fields containing more than 2,000 audited entities’ data that must be compared in order to be certain of the fairness of existing financial transactions; as a consequence, the given parameters become more complex.

My point here is to emphasise the fact that, during the matching process, we can see how human involvement in the decision making process could be replaced by a computer system, in relation to the classification and analysis of various types of audit data.

Further, Justice Ginsburg’s writing about Arizona v Evans (1995) reveals her skepticism about the computer system: “Computerization greatly amplifies an error’s effect, and correspondingly intensifies the need for prompt correction; for inaccurate data can infect not only agency, but also the many agencies that share access to the database” (as cited in Steinbock, 2005, p. 54).

The above conditions explain to us that if the information that is matched is not accurate and the matching process itself is not reliable as a system, these issues will influence the conclusions drawn about the matching result and influence a decision’s level of accuracy. However, the extent to which this phase threatens privacy depends on the nature of the decision; the privacy threat will be more significant for decisions that involve individuals, for example, in investigations of corruption cases.

3. The auditors’ judgements on personal profiles: a threat for the “output”

So far, I have discussed the input and output from the data matching system and have noted that the last phase of e-Audit’s data matching system is the output. According to Chapter 2, we know that the final results of this data matching system are personal profiles and/or organizational profiles. Reaffirming my statement at the beginning of this chapter, this part of my discussion will focus on personal profiles.

First of all, it is important to note that personal data in an audit process functions as supporting documents. We can also say that personal data are part of the audit data. The illustration below describes how personal data becomes part of the audit documents.

---


173 Office of The Information and Privacy Commissioner/Ontario: 39

174 Steinbock, 54.
One financial audit method instructs auditors to do a “substantive procedure”\(^\text{175}\) in order to detect material misstatements in the existing transactions. Therefore, the auditors are required to verify information from a financial statement, including its supporting documents. For instance, an auditor may verify the expenditure account from a financial statement. At that time, the auditor for example suspects that there is fraud in the travel expenses office. One way to get a reasonable assurance is by comparing the existing documents with the list of passengers’ names from the related airlines. In this case, personal data function as supporting documents in order to assist the auditors in analysing and formulating the audit documents into the audit report.

Based on the above illustration, I believe that for every type of audit\(^\text{176}\) the Audit Board will deal with the data matching system in order to analyse the audit documents. Therefore, in Chapter 2, I stated that the results of the data matching system will contribute before, during and after an audit process.

Before we discuss into more detail about how the auditors work with the output of the data matching system, I will explain how the international standard assigns the auditors in performing the audit duty. Paragraph 14 of INTOSAI’s “Basic Principles in Government Auditing” reminds the auditors that “to ensure that high quality work is done, appropriate standards must be followed”.\(^\text{177}\) Further, paragraph 29 states that auditors can use their judgement in performing an audit, considering that the auditing standards are the minimum requirements for an audit process.\(^\text{178}\)

However, this document is only a basic guideline for members of the INTOSAI. Therefore, applying the auditors’ judgements as part of the audit standard will depend on the policies of every INTOSAI member, because they come from various countries that have different policies for regulating their standards. The Audit Board obliges the auditors to use their professional judgement during the planning phase, the auditing phase and the reporting phase of an audit process.\(^\text{179}\) Moreover, in paragraph 27 of the financial audit standard (PSP 02), we find that the auditors’ judgement may also be used to measure the quantities, types and contents of the audit documents.\(^\text{180}\)

\(\text{\textsuperscript{175}}\)See supra note 72.
\(\text{\textsuperscript{176}}\)See supra note 14.
\(\text{\textsuperscript{178}}\)Ibid., 6.
\(\text{\textsuperscript{179}}\)Peraturan BPK RI Nomor 01 Tahun 2007 tentang Standar Pemeriksaan Keuangan Negara <the Audit Board Regulation Number 01 Year 2007 concerning Standard of Auditing of Public Finances, my own translation> The preliminary of The Audit Standard, Paragraph 27: 18.
\(\text{\textsuperscript{180}}\)Ibid., paragraph 27: 42 < my own translation>.
Based on the above explanations, we already have a clear description of how an auditor’s judgement is applied in Indonesia. Nevertheless, a problem might arise when paragraph 30 of the general standard requires the auditors to use “a ‘professional skepticism’ that implies, in performing an audit, the auditors must have an attitude that includes a questioning mind and a critical assessment of audit evidences.”\textsuperscript{181}

We recognize that the output of the data matching system is personal profiles that function as supporting documents that will automatically be audit evidence in an audit process. Now, we discover that the auditors’ judgements are required to stipulate “professional skepticism”. It seems to me that the auditors’ “professional skepticism” about personal profiles has the potential to generate “profiling”.

Profiling is “the process of discovering correlations between data in databases that can be used to identify and represent a human or nonhuman subject (individual or group) and/or the application of profiles (sets of correlated data) to individuate and represent a subject or to identify a subject as a member of a group or category.”\textsuperscript{182}

Based on the above definition, in my opinion, profiling happens regardless of the number of personal profiles that are created and does not merely identify a person or a group in a direct way. In the meantime, according to Hildebrandt (2008), profiling has a wider definition because it relates to the people, things or situations that relate to a person or a group.\textsuperscript{183} Moreover, the related things and situations can be used to assess the possible opportunities or risks that are attached to the person or group.\textsuperscript{184} Basically, the main objective of using personal profiles as the output of the data matching system is to support the auditors in formulating the audit report. However, how the auditors utilize personal profiles will differ from one auditor to another. I must re-emphasize the importance of paragraph 27 of the Financial Audit Standard (PSP 02) which stated that auditors’ judgements can be applied to measure quantities, types and contents of audit documents.

In my view, paragraph 27 PSP 02 is a subjective standard, as I believe that every auditor will have different ways for measuring the adequacy of quantities, types and contents of audit documents. Therefore, in my opinion this condition could result in one of two possibilities when auditors deal with personal profiles:

\textsuperscript{181} Ibid.,30 <my own translation>.
\textsuperscript{182} Schermer,45.
\textsuperscript{183} Hildebrandt, Profiling The European Citizen, 303.
\textsuperscript{184} Ibid.
1. One possibility is that, based on the auditors’ (professional) judgement, the existing personal profiles are considered adequate for direct use in an audit report without further analyses.\textsuperscript{185}

2. A second possibility is that, based on the auditors’ judgement of the existing personal profiles, the profiles will be deemed to require more detailed elaboration.

With respect to the first possibility, I do not approve of auditors using personal profiles directly as output for the data matching system to support an audit report. My argument is that an automation process using a computer system is clearly nothing more than an artificial intelligence that will have inherent errors in its matching process. Furthermore, the algorithms will grasp correlations from among personal information “without establishing causes or reasons.”\textsuperscript{186} This means that the accuracy and validity of the profiles are unreliable.

For example, suppose that the output of a matching process provides a personal profile of a suspect in a corruption case, revealing that the suspect’s monthly income is bigger than his official monthly salary as a public officer. The immediate judgement of the auditors will be that there are strong indications that the suspect is corrupt and they will use the information in the audit report. This may have been otherwise if the auditors were to analyze the profiles and elaborate upon them with existing relevant data; these may reveal another reason why the suspect’s income is larger than his official salary: for example, the suspect has a job on the side.

My concern for the second point is when the auditors’ judgements play roles in their “professional skepticism” through profiling that develops “new knowledge” about the individuals. New knowledge about a personal profile is built when the auditors assess the profile through elaborating the profiles based on their judgement. We have to underline here that using auditor’s judgements to elaborate the profile is not always bad, as long as the auditors are not excessively analysing the profile beyond the context of the audit. However, if the auditors judge personal profiles more elaborately and build new knowledge without confirming with the individuals before the profiles are processed further,\textsuperscript{187} auditors do interfere with individuals’ privacy. For example, new knowledge may arise if auditors assess personal data with unrelated data in an audit, such as in an audit in order to investigate a “mark-up”\textsuperscript{188} case on utilising health insurance.

\textsuperscript{185} “Analysis is “the process of breaking a complex topic or substance into smaller parts to gain a better understanding of it.” \texttt{http://en.wikipedia.org/wiki/Analysis}. As cited on September 9, 2012.

\textsuperscript{186} Hildebrandt, Profiling The European Citizen, 18.

\textsuperscript{187} The Audit Board Regulation Number 01 Year 2007, paragraph 32, in General Standard (PSP01), for certain conditions, the auditors are able not to apply certain standards, but they must be disclosed the reasons in the audit report.

\textsuperscript{188} “Mark-up” means to increase the price of goods or services above the market price, even though the actual payment is less, and then take advantage of the price, i.e., the actual price of a box of pens is
Based on the existing Indonesian regulations, members of The House of Regional Representatives are covered by health insurance that provides reimbursement or care provisions that are available in government hospitals. It should be borne in mind that in Indonesia, most commercial and service transactions up to a certain amount are usually paid in cash, so the possibility exists that the auditors were unable to analyse proof of the suspect’s financial transactions.

Furthermore, the existing personal profile of the suspect provides information concerning the receipts of several payments, e.g., for medicines, laboratory tests, doctors’ consults, etc. Based on the auditor’s judgement, if these data do not adequately convince him that the suspect really needed all the treatments and that all the payments really took place, the auditor could elaborate on the medical treatment results, e.g., requesting laboratory test results and other evidence of medical treatment in order to carry out further analysis of the “mark-up” case. It is common in auditing processes to apply the “apple to apple” comparison method in a “mark-up” case.

My point here is to emphasize that elaborating on evidence of medical treatments is already encroaching on a suspect’s privacy and is not directly related to the audit context. Accessing evidence of medical treatment will supply the auditor with new detailed knowledge regarding the suspect’s illnesses. I regard procedure confirmation by related hospitals as a better alternative for supporting an audit report.

Furthermore, as I explained previously, one of the structures of an audit finding in an audit report is the “condition”, which consists of information based on facts. The ways in which an auditor structures conditions in a mark-up case for an audit report presents possibilities for disclosing (either explicitly or implicitly) any diseases the suspect may have.

Profiling may inevitably influence the auditors while formulating the audit report. The personal profiles will build a specific description about certain personalities. As I stated in Chapter 1, personal profiles provide auditors with insight, so they can form a premature description of certain individuals. For instance, if personal profiles suggest that a certain individual spends an amount of money every month that exceeds the amount of his income. This will lead an auditor to suppose that this person has a strong motive to commit fraud.

The demand of “professional skepticism” causes the auditors to further elaborate about their judgements of the profiles. However, various factors will influence the auditors in judging these personal profiles: educational backgrounds, social value, cultural value and intelligence level play significant roles in interpreting the profiles.

Rp5.000,00, but the report states Rp8.000,00, and the rest of the money (Rp3.000,00) is as the amount of the “mark-up”.

Apple to apple comparison method is one of the audit method in public loss cases by comparing certain goods or services that are similar.
Johnson-Laird (1983), a professor of psychology, developed a mental model theory that “posits individual to make inferences by constructing and integrating mental model, which are internal (mental) representations of some external state of affairs.”\(^{190}\) In other words, a mental model is an illustration of an individual’s opinion concerning a condition.\(^{191}\) Furthermore, according to Veer and Melguizo (2003), “mental models are constructed from perception, imagination, of comprehension of discourse” (as cited in Jansoon, et al, 2009, p. 147).

Adams (n.d.) claims that mental models “play a central and unifying role in our conception of the world and enable us to predict and interact with it.”\(^{192}\) She analogizes a mental model in a restaurant: “what is expected to be found (e.g. food, tables), to occur (e.g. ordering food and eating food), and how we should behave (e.g. table manners).”\(^{193}\) For those reasons, in relation to the impact of profiling, I agree with Hildebrandt’s opinion (2008) that states: “profiling is a knowledge construction and it produces new kind of knowledge about groups or individuals.”\(^{194}\)

I mentioned several times in this chapter that personal profiles that consist of personal information reflect the individuals' identities as part of their dignity, respect and integrity. In the meantime, “identity is the core of privacy”,\(^{195}\) where privacy is a fundamental right of the individual. Therefore, basically, no one can interfere with personal profiles through adding, removing, judging and building new knowledge into personal profiles. Personal profiles belong to the individuals and only they have the right to do anything to their profiles.

However, under certain conditions privacy may be overruled. The first condition is for the public interest, for instance, when dealing with terrorism in a country. Usually, several intelligence techniques (such as interception) are used in order to get relevant information. The second condition is in the workplace. In the EU\(^{196}\) and the USA\(^{197}\), employers are able to access their employees’ email or to use CCTV in certain places as a way of monitoring their employees, as long as the employees have been informed about these practices. It should


\(^{193}\)Ibid.

\(^{194}\)Hildebrandt, Profiling The European Citizen 303.

\(^{195}\)Hildebrandt, Privacy and Identity 7.


be noted that though these exceptions do exist, there are still limitations in practice, such as having sufficient reason to act, informing data subjects when possible, and ensuring that processed data are correct.

The threats to privacy are more clear when new knowledge of personal profiles are used as supporting data in the audit report. We know that the audit report of the Audit Board constitutes an administrative decision of the public body. It is similar to other administrative decisions, the audit report is legally binding through its recommendations.

As previously stated that the recommendations of an audit report provided by the Audit Board must be followed up on by the government officers and third parties. The implementation of these recommendations is guaranteed by the law, through imposing the fine under the penal code for government officers who do not obey the law. The types of recommendations that will be provided depend on the audit findings: they might be administrative, indemnification or legal proceedings.

In addition, the Audit Board has the obligation to submit the audit report to third parties and to publish it publicly. We can imagine the effects on the individuals if this “new knowledge” reveals “negative” information about the individuals that are contrary to the facts. How will people think about you if your name is mentioned as one of the parties who are involved in a project that is accused of a criminal act with regard to state finance management in the audit report? Where is the principle of “presumption of innocence”? Additionally, what about a case in which personal information that must be concealed is customarily revealed in an audit report? Such conditions will definitely cause inconvenience, not only for the person involved but also for his family. As stated by Schwartz (2004), the processing of personal data by public bodies will have consequences to the choices that we make.

3.4 Conclusion

As we all know, privacy is one of the fundamental rights of human beings that must be protected as being based on humanistic values relating to the concept of privacy. Bearing in mind that privacy consists of humanistic values, then clearly everyone has the right to control their personal data.

However, the development of information and technology that provides speed and convenience may make it difficult for individuals to control the flow of their personal data. In addition, the absence of a clear and comprehensive legal framework may result in a threat to people’s privacy.

---

198 Presumption of innocence is a principle that one is considered innocent until proven guilty (<http://en.wikipedia.org/wiki/Presumption_of_innocence>). As cited on July 30, 2012.
The implementation of the data matching system in e-Audit, which uses the IPO model approach, enables us to identify threats in every element of the system. The first is of these is “re-using personal data”, which is a threat in the input phase. The implementation of e-Audit requires information sharing among audited entities for “cross-checking purposes” through online communication. However, this information sharing is not accompanied by obtaining consent or informing the data owners. The absence of data owners’ participation regarding the processing of their data may lead to inaccuracies and invalidity of the personal data being processed. It should be borne in mind that the data owners are not fully aware of what has been done with their personal data; they do not even know the extent to which their personal data could impact their lives negatively as a result of inaccuracies and invalid data.

The next threat, “computer matching”, takes place during the process phase. We are aware that algorithms play a significant role during the matching process for identifying the interrelationships between personal data. The ability of algorithms to identify “hits” is supported by the computer system. Nevertheless, this “artificial intelligence” does in fact involve an inherent risk that could result from either the hardware or the software. For instance, problems with duplicates in a data set may occur during the matching process which could result in inaccurate and invalid personal profiles.

The last threat is the auditors’ judgement on personal profiles which is a threat during the output phase. In this stage, the existence of auditors’ judgement could result in the following conditions: (1) the auditors rely too much on the output of the matching system, and (2) the auditors elaborate on the profiles excessively. The first condition could result in a premature decision, while the second refers to situations in which the auditors could be interfering in the privacy sphere of the data owners.

In this section, my identification results suggest that every phase of the matching system involves a threat that could compromise the data quality. As I mentioned before, personal data, as part of the audit data, will be used to support the audit report. If the personal data used are invalid and inaccurate, then the excessive disclosure of personal information in an audit report may inevitably threaten privacy. The Audit Board is under an obligation to publish the audit reports and carry on processing audit findings that have indications of corruption, which could eventually result in legal proceedings.

To sum up, I must emphasize that technology, data quality and a clear and comprehensive legal framework are interconnected in the field of privacy and data protection.
CHAPTER 4– Legal Analysis of the Threats to Privacy

4.1 Introduction

The conclusion to Chapter 3 stated that there is a relationship among technology, data quality and a clear and comprehensive legal framework. That conclusion is based on the identification result in data matching system in e-Audit. However, we already determined that the main issue of the data matching system is “the quality of personal data”. Now, we will discuss how the issues that arise during the identification process described in Chapter 3 are correlated with the Indonesian legal framework.

The purpose of this chapter is to analyze how well the Indonesian legal framework responds to threats to privacy related to the data matching system in e-Audit. However, the beginning of this chapter will discuss Indonesia’s involvement in OECD and APEC and will give insight into how Indonesia has developed its legal framework around privacy and data protection.

To avoid an exhaustive analysis, the discussion will be focused on the issues that are related to “quality of personal data”. Furthermore, we will discuss at a glance “data quality” issues within the EU legal framework. The approach in the EU legal framework is used for two reasons: (1) some of the EU Member States are part of the top 20 world e-government development leaders in 2012; and (2) the EU is one of the global potential markets for Indonesia. In addition, a European case will be presented in this chapter, in order to correct the misconception that public bodies do not have any limitations in processing personal data.

4.2 The Indonesian legal framework

4.2.1 General

The Indonesian legal system is based on the combination of civil law and customary law. Hence, “written law” or “codification” is the primary source for the Indonesian legal system. Furthermore, we will see how far privacy exists in the Indonesian legal framework.

The 1945 Constitution is the basis for other regulations in Indonesia, and Pancasila is the country’s philosophical foundation. The 1945 Constitution and Pancasila both embody “humanitarian rights and freedom that derive from old traditions, custom and philosophy of life of the Indonesian people”.

Pancasila consists of five principles: “belief in the one and only God, just and civilised humanity, the unity of Indonesia, democracy led by the wisdom of deliberations among

---

200 See supra note 38.
representatives, and social justice for the whole of the people of Indonesia.” These five principles reflect the values in The Universal Declaration of Human Rights.

One of the characteristics of a modern state is recognition of human rights in the constitution. The concept of human rights has a meaning about the standard of humanitarian values that must be protected and are universally applicable. The main reason why the 1945 Constitution mentions the value of human rights is as a declaration that the Indonesian government will guarantee protection of human rights in Indonesia.

The other concept that was adopted by Indonesia in relation to the issue of human rights is the concept of democracy. The concept of democracy provides a foundation for a mechanism of an authority based on the principle of equality among human beings. This means that Indonesia respects the sovereignty of its people, including their personal rights.

In addition, in a democratic environment there is a demand for individuals to participate by getting involved in the state’s administration affairs. The involvement of individuals in a democratic environment is indicated through general elections, registration of personal data through an online application and other obligations that relate to the utilization of information technologies. Therefore, in the era of information, the participation of individuals in the government sector requires the individuals to share a lot of their personal data with the government through the utilization of technologies. We know that kind of participation will accelerate the realization of good governance in Indonesia, but it does not mean that the realization of good governance prescribes the individuals to pay for it with their privacy rights.

I mentioned before that Indonesia does not fully implement to the Universal Declaration of Human Rights, but they have several similar principles, specifically for humanitarian issues such as: right to life (article 28A), equality before the law (article 27) and freedom of thought and freedom of religion (article 28E). The most important articles for this research are articles 28F and 28G of the 1945 Constitution. Even though both of the articles only

---

203Ibid.
206Undang-undang Dasar 1945 (The 1945 Constitution) article 28F: “Every person shall have the right to communicate and to obtain information for the purpose of the development of his/her self and social environment, and shall have the right to seek, obtain, possess, store, process and convey information by employing all available types of channels.” <http://www.wipo.int/wipolex/en/text.jsp?file_id=200129>. As cited on June 4, 2012.
207Undang-undang Dasar 1945 (The 1945 Constitution) article 28G: “(1) Every person shall have the right to protection of his/herself, family, honour, dignity, and property, and shall have the right to feel secure against and receive protection from the threat of fear to do or not do something that is a human right. (2) Every person shall have the right to be free from torture or inhumane and degrading treatment, and shall have the right to obtain political asylum from another country.” <http://www.wipo.int/wipolex/en/text.jsp?file_id=200129>. As cited on June 4, 2012.
implicitly mention privacy and its protection, the values of privacy and its protection already exist in the 1945 Constitution.

We know that privacy is a fundamental right that contains the values of dignity, integrity and respect for individuals. Therefore, privacy has to be protected through the protection of personal data. I believe privacy issues so far have not been very significant in the Indonesian society that has a strong communal background. However, the invasion of information technologies will impact and shift the values in Indonesian society towards a global community.²⁰⁸

It has been said that privacy is one of the fundamental rights that consist of humanistic values. Therefore, even though Indonesia and the EU have different concepts of privacy, I believe basically that values relating to privacy, which involve such aspects as human dignity, are universal. It seems to me that suggesting that the problem relates to different concepts is in fact a misinterpretation of how Indonesian people interpret the concept of privacy, because:

1. as I stated before, Indonesian people have a strong communal background, but I believe the existence of a communal background does not mean that we are willing to disclose all our personal information to society at large. I believe that having a private sphere is a basic human need of every human being.²⁰⁹

2. information technology has not been applied as widely in Indonesia as in Europe. Consequently, an abundance of privacy cases, which often arise due to the impact of the development of information technology, is not generally echoed in Indonesia. It seems to me that this is also one of the reasons for the different interpretation of privacy between Indonesia and the EU.

Based on the above reasons, it is possible that Indonesian people have not yet realized that privacy is a valuable aspect of human rights and one that must be protected. Nevertheless, I believe that, as part of a global community, especially with respect to international trading and the invasion of information technology, Indonesia will gradually be forced to alter its concept of privacy.

One issue that indicates a shift in Indonesian society is the involvement of Indonesia in international and regional organisations that contribute to developing Indonesian laws pertaining to privacy and data protection. The Organisation for Economic Co-operation and Development (OECD) guidelines on The Protection of Privacy and Transborder Flows of Personal Data is one of the non-binding international instruments in privacy and data

Though Indonesia is a non-member economy of OECD, it has working relationships with OECD member countries, so in 2004 Indonesia signed the guideline and further ratified it. Eight basic principles from the guideline should be applicable to national legislation: (1) collection limitation; (2) data quality; (3) purpose specification; (4) use limitation; (5) security safeguards; (6) openness; (7) individual participation; and (8) accountability.

Further, to strengthen trade cooperation between Asian-Pacific countries, Indonesia officially joined the Asia-Pacific Economic Cooperation (APEC) in November 1989. To enable privacy protection across the member economies in the APEC region, ministers endorsed the APEC Privacy Framework in 2005. This framework has nine principles: (1) preventing harm; (2) notice; (3) collection limitation; (4) uses of personal information; (5) choice; (6) integrity of personal information; (7) security safeguards; (8) access and correction; and (9) accountability.

As part of a global community, the demand for international trading by utilizing IT forces Indonesia to adapt its national regulations. The astonishing invasions and the rapid developments of technologies will inevitably impact Indonesian society and shift the concept of privacy in Indonesia.

### 4.2.2 Regulation of privacy

Since 2008, Indonesia has stipulated Law Number 11 Year 2008 concerning Information and Electronic Transactions. This regulation constitutes a milestone for the legal admissibility of electronic transactions in Indonesia, and particularly the recognition of protection of personal data as part of privacy rights. In order to get a structured discussion, next we will discuss Law Number 11 Year 2008 and a number of other laws that are somehow related to privacy in the context of the Indonesian legal framework.

I will divide my analysis into two parts: (1) “consent” and “informing”, to analyze the threats to privacy for the “input” and “output” phases; and (2) technology and human involvement, for the threats both during the “process phase” and for “the output”. In my opinion, those two points have a strong relationship to the quality of personal data.

---

210 <http://www.oecd.org/document/18/0,3746,en_2649_34223_1815186_1_1_1_1,00.html>. As cited on June 4, 2012.

211 <http://www.oecd.org/document/13/0,3746,en_33873108_39418603_40743181_1_1_1_1,00.html>. As cited on June 4, 2012.


213 <http://www.oecd.org/document/18/0,3746,en_2649_34223_1815186_1_1_1_1,00.html#part2>. As cited on June 4, 2012.


1. “Consent” and “informing”

Now we will see how Indonesian regulations accommodate those issues. Law Number 39 Year 1999, concerning Human Rights, is a starting point for my analysis. We already know that as the basic norm for other regulations in Indonesia, the 1945 Constitution does not explicitly mention the existence of privacy and data protection. However, based on the Indonesian Constitution, we know that the values exist in Indonesia, and it is re-emphasized in article 29 (1) of Law Number 39 Year 1999:

“Everyone has the right to protection of the individual, his family, opinion, honor, dignity, and rights.”

My first point here is to underline that the protection of privacy values already exists in Indonesia.

Next, we will see how these values are implemented on practical levels. For this purpose, I present several related articles in Indonesian regulations:

Article 21 Law Number 39 Year 1999, concerning Human Rights:

“Everyone has the right to integrity of the individual, both spiritual and physical, and as such shall not become the object of any body research without his approval.”

Article 47 (1) Law Number 8 Year 1981, concerning the Criminal Procedure:

“...the authorized investigators have authorities to open and to check personal mails that are sent by post and telecommunication offices, if there is a legitimate reason and previously must obtain specific permission from the head of the national court.”

Article 40 of Law Number 10 Year 1998, concerning Banking:

“A bank has an obligation to conceal personal data from its customers, except for public interests (taxation and law enforcement). The order to disclose personal data of customers is given through the Head of the Indonesian Central Bank with the approval of the Ministry of Finance.”

Further, Article 44 A (1) states:

“Based on a written request and the approval or authority of a customer, a bank is obliged to provide other banks that are referred by the customer with information pertaining to the savings of that customer.”

Article 26 (1) Law Number 11 Year 2008, concerning Information and Electronic Transactions:

218 Ibid.
219 <my own translation>.
220 The summary of article 40 jo. 41, 41A and 42 of Law Number 10 Year 1998 <my own translation>.
221 Article 44A (1) Law Number 10 Year 1998 <my own translation>. 
“Unless provided otherwise by laws and regulations, use of any information through electronic media that involves personal data of a person must be with the consent of the person concerned.”

From the above articles, we know that the Indonesian legal framework respects the rights of individuals to control their personal data through giving their “consent”. However, as I stated earlier, privacy rights can be more flexible under certain conditions or for reasons of public interests. It means that as long as there is a legitimate ground, the processing of personal data does not require consent from the individual.

Further, the issue of re-use of personal data arises when a bank can provide their customers’ personal data for public interests without informing the customers or providing a mechanism that allows individuals to update their personal data. Therefore, the concept of the issue of re-using customers’ data in banking is the same as the concept stated in article 26 (1) Law Number 11 Year 2008. This means that, for public interest, consent and informing are not required.

So far, I have not found any crucial limitations that protect privacy rights from the invasion of public bodies utilizing personal data except Article 17(h) Law Number 14 Year 2008, concerning The Disclosure of Public Information:

“Every public agency is obliged to provide access to obtain public information for every public information applicant, except Information that if disclosed and supplied to public information, applicant may reveal a personal secret, ie:

(1) the history and condition of a member of the family;
(2) the history, condition and care, physical medical treatment, and physic of an individual;
(3) the financial condition, assets, income and bank account of an individual;
(4) evaluation results of the capability of an individual; and/or
(5) personal notes of an individual pertaining to his/her formal education and non formal education activities.”

Based on the above discussion, it seems to me that, firstly, Indonesian regulations defining privacy are limited because the scope of privacy is only limited in Article 17(h) Law Number 14 Year 2008, but also by article 26 (1) Law Number 11 Year 2008. Secondly, it is my view that, as the most up-to-date regulation, Law Number 11 Year 2008 should be more responsive to personal data protection issues in the context of development of information technologies.


Furthermore, the following discussion focuses on “informing” individuals. There is general recognition for the fact that “consent” in relation to matters of public interest is not required in processing personal data. For this reason, I believe I have been clear about the discussion of “consent” in my research.

We can all agree that re-using personal data in the matching system is important for improving the Audit Board’s performance, as it will contribute to improving the monitoring of state finances for the benefit of the public. Unfortunately, this condition is not balanced by further mechanisms on how to protect personal data. This information asymmetry may form a threat to the quality of data relating to personal information. Therefore, in my opinion, it is necessary to shift the balance of personal information by incorporating into the Indonesian Legal framework several related principles from both the APEC and the OECD that were mentioned previously.

The first of these is the “notice” principle. This principle is one of eight principles of the APEC privacy framework on protecting personal data. Basically, what it means is that data-owners have the right to be informed about the collection, the purpose and the disclosure of their personal data. With regard to implementing the data matching system within the context of e-Audit, I realize it would be impossible, considering the numbers of audited entities and the frequency of the audits that are performed – to inform every data owner at every phase of the data matching system. Therefore, it seems to me that notice should at least be given to data owners about whom strong indications already exist, thereby making them a suspect in a corruption case. This amounts to giving notice in the last phase of the data matching system. For the rest, the APEC privacy framework provides no further information on what form the “notice” should take (written or oral).

The second is the “collection limitation” principle. This principle is incorporated both into the APEC privacy framework and that of the OECD. This principle stresses limiting the collection of personal data according to the purpose of that collection, and obtaining data legally and fairly.

I shall not, at this stage, discuss any further matters relating to consent, but will limit myself to the collection itself.

As I see it, this principle prescribes that, in order to prevent the abuse of personal data, the Audit Board should delete all personal data that have not already been used from BPK’s data center, based on rules relating to the retention of the personal data. This does not mean that after the auditors have finished performing a certain audit type, the auditors will delete all related personal data. On the contrary, these personal data will be stored until the end of the storage time. It should be borne in mind that audit data, including personal data will usually be used in court as audit evidence, particularly in cases involving corruption and

bribery. Therefore, considering my explanation regarding the retention of personal data, it seems to me that the principle of “collection limitation” in this sense is related to the principle of the OECD’s “use limitation”.

If this were to take place, the Audit Board will be required to design a system for retaining personal data in order to measure personal data storage time. The timetable for implementing e-Audit (in Chapter 2) shows that the Audit Board designed SOP for data retention and data deletion. However, SOP is still in the process of being developed.

The next principle is “data quality”. This is one of the OECD principles that regulate the relevancy issue in processing personal data. However, this principle also regulates the accuracy and completeness of personal data and the fact of their being constantly up-to-date, which are basic requirements in connection with the extent to which personal data are (re-) used.226

“Access and correctness” is the fourth principle that should be considered for adoption into the Indonesian regulation. In my opinion, this APEC principle plays the most important role, not only with respect to enforcing data-owners’ rights to their personal data, but also with respect to the accuracy and validity of the audit data that will directly impact the credibility of the Audit Board through its audit reports. Furthermore, this principle provides data-owners with the opportunity of maintaining their dignity, their self-respect and their integrity.227

With regard to the data matching system in e-Audit, my point is to describe how, by adopting the principle of “access and correctness”, the data owners are provided with knowledge regarding the processing of their personal data. It is assumed that the Audit Board will give data owners an opportunity to access their data in order to correct or update their personal data before these personal data are used to support an audit report, moreover before the audit report is handed over to the law enforcement agencies. I believe, in a democratic society, that this principle contributes more, because it mitigates asymmetric information between public bodies and data owners and makes use of “due process”228, so data owners have the opportunity of knowing what is happening to their data.

Previously I stated that generally, in order to support the government programs, the government requires personal information from its citizens. Specifically in a democratic

228Due process is a legal guarantee that someone will be given notice of the proceedings and an opportunity to be heard before the government acts to take away one’s life, liberty, or property. <http://legal-dictionary.thefreedictionary.com/Due+Process+of+Law>. As cited on September 21, 2012.
society, where the participation of individuals in public sectors is reflected by handing over their personal data to the government agencies.

With regard to the implementation of e-Audit, the Audit Board requires personal data in order to support a better monitoring system of management and accountability of state finances. Tax number (a kind of social security number), personal bank account, certificate of asset ownership are several related personal data that are used in order to detect any mismanagement or fraud in managing state finances.

Remembering the value that exists in personal data, under Law Number 15 year 2004, article 10 (a) and (b), and Law Number 15 Year 2006, article 9(1) point “b” and “d”, and article 9 (2), the Audit Board has legitimate grounds to access personal data. However, It should be underlined, that even under legitimate grounds, there should be safeguards for the data owners to protect their personal data from unlawful processing.

Therefore, in the context of data matching process in e-Audit, informing the data owners at the last phase of the matching system, based on my opinion is the most effective way to maintain the data owners’ rights on their personal data.

To emphasize my analysis, I use Birnhack’s (2008) analogy.\(^{229}\) in intellectual property rights, the rights holders can transfer the rights to other parties without maintaining the rights. Conversely, considering the values that exist in personal data, individuals will keep maintaining their rights for any type of processing. This right remains even though individuals already gave consent or precisely authorized their personal data to be processed by the government, in consideration of improving the welfare of its citizens.

To sum up this section, I believe, there should be further mechanisms that regulate the issues that relate to processing personal data, particularly the “re-using” issue and the disclosure to public as a form of transparency through a clear and comprehensive legal framework. It is a contradiction that Indonesia has a complete regulation concerning the rights of individuals to their properties (both in Law Number 14 Year 2001, concerning Patents, and Law Number 6 Year 1982, concerning Copyrights) but the nation does not have any complete and comprehensive regulation regarding data protection. I shall therefore discuss, summarily, some countries that are rather similar to Indonesia in respect to e-government where privacy and data protection already exist:

(1) Malaysia

Malaysia has a specific regulation on data protection, namely: Personal Data Protection Act 2010. This act is limited to regulating the processing of personal data of individuals only in commercial transactions in the private sector.\(^{230}\) However, this act was influenced mostly by the EU Data Protection Directive (Directive 95/46/EC) , rather than

---

\(^{229}\) Birnhack, 3.

by the OECD guidelines or the APEC Legal Framework. 231 Seven principles of the Act are: 232 (1) general principle, (2) security principle, (3) access principle, (4) notice and choice principle, (5) disclosure principle, (6) retention principle, and (7) data integrity principle.

(2) Philippines

The Philippine Senate enacted the Data Privacy Act of 2011 on 20 March 2012. 233 This act covers both public and private sectors. 234 The purpose of collection must be declared before collection, and collection limitation, subsequent use and disclosure or other processing required must be declared as soon as the data subject has given express or implied consent. 235

2. Technology and human involvement

As previously mentioned, these issues aim to respond to the threat to privacy during the matching process and for the output phase. Article 15 Law Number 11 Year 2008, concerning Information and Electronic Transactions, implies that:

“Any electronic system provider must provide electronic systems in reliable and secure manner. Moreover, they have to be responsible for their electronic system, except when there are faults and/or negligence on the part of electronic system users.” 236

In my view, this law already addresses technical issues and prescribes that any parties that perform electronic data processing must fulfil the minimum requirements. 237 It means that this law requires parties that process data electronically to provide a reliable system.

Furthermore, we will discuss how Indonesian regulations regulate the issue of reliance on technology. Based on Law Number 39 Year 1999, concerning Human Rights, and Law Number 36 Year 1999, concerning Telecommunication. Article 3(1) Law Number 39 Year 1999 states:

---

233 Ibid., 2.
234 Ibid.
235 Ibid., 3.
237 Shortly, article 16 Law Number 11 Year 2008 stated that the operation of electronic system at least complies with the requirements: can redisplay the electronic information, can protect the availability, entirety, authenticity, confidentiality, and accessibility of electronic information, comply and furnished with procedures or guidelines, and adopt sustainable mechanism. <http://www.cgap.org/gm/document-1.1.6079/INDONESIA%20Law%20OF%20TRANSACTIONS.pdf>. As cited on July 15, 2012.
“Everyone is born equal in dignity and human rights, and is bestowed with the intellect and reason to live with others in a spirit of brotherhood.”

Article 2 Law Number 36 Year 1999 states:

“Telecommunication is performed based on the principles of utilization, fairness, legal certainty, partnership, ethics, and self confidence.”

In this section, my discussion focuses on the nature of a human being and a new issue in my research: “ethics”. My discussion starts with a statement made by Jacques Ellul:

“... the danger of what might happen to our humanity in the present half-century, and distinguishing between what we want to keep and what we are ready to lose, between what we can welcome as legitimate human development and what we should reject with the last ounce of our strength as dehumanization.”

I must emphasize here that a human being has a “brain” capable of distinguishing between “bad” and “good” and the capacity of improving his life through innovation. Technology does a lot to human beings, but as human beings we are able to distinguish impacts that arise from the existence of technology.

One product of human innovation is the computer system. Actually, a computer is merely a machine that a programmer instructs to do certain activities. In other words, this “artificial intelligence” was created by a human being.

Article 2 Law Number 36 Year 1999 mentions “ethics”. Ethics is known “as moral philosophy is a branch of philosophy that involves systematizing, defending, and recommending concepts of right and wrong behavior.” According to Spinello (1995, p. 14), the purpose of ethics is to help us behave honourably and attain those basic goods that make us more fully human.

My point here is to underline that, as I stated before, technology can improve our life, but it does not mean that we do not need allow human beings to assess the output of technology through their abilities. In the case of the data matching system, I think it is not fully human to rely solely, without reflection, on personal profiles as the output of the matching system, thereby constructing new knowledge about certain individuals based on the information in their profiles. A human being should treat technology as a tool but continue to use his

---

239 <my own translation>.  
intelligence in analyzing information from profiles before making a decision. The analyzing process is required based on the existing context.

4.3 Lessons from the EU

In this section, we will see how the EU legal framework responds to the issues of data quality. Data protection in the EU is regulated through Directive95/46/EC, on The Protection of Individuals With Regard to The Processing of Personal Data and On The Free Movement of Such Data. Directive 95/46/EC was adopted by The EU. The European Court of Justice (ECJ) has important roles in its interpretation. However, besides this Directive harmonize Data Protection Law within The EU, this Directive also has a global impact. Swire & Litan (1998) and Bennett & Raab (2006) imply that “The EU Directive on Data Protection (1995), which came into force in 1998, is the most comprehensive and successful international instrument of data protection laws” (as cited in Birnhack, 2008, p.8).

First of all, I need to inform the basic concept of personal data based on Directive 95/46/EC. Article 2(a) of this directive defines personal data as “identified” or “identifiable.” In addition, Directive 95/46/EC has principle of “data quality,” that regulated in article 6(1). The issues pertaining to the “data quality” principle are:

1. fairly and legally processed, measuring fairness will depend on the country’s interpretation. Legally means that personal data must be processed based on the existing regulations;
2. purpose limited: personal data must be processed for a specific purpose and not for further processing;
3. relevant: it means, processing personal data must be adequate and not excessive;
4. accurate: personal data must always be accurate and kept up to date;
5. time limited: personal data must be kept not longer than is necessary.

---

With regard to the automation process, it is significant to inform that according to Article 15 (1) Directive 95/46/EC states that “Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.”

Further, article 15 (2) of the Directive allows a person, subject to article 15 (1) with conditions, to enter into a contract, as long as adequate safeguards to protect his legitimate interests are governed by law.

In addition, concerning to the issue of re-use of personal data, actually the EU has Directive 2003/98/EC on the Re-use of Public Sector Information. However, in my opinion the concept of this Directive is quite different with the topic that we discuss. This Directive is more for commercial purposes, and it does not regulate pertaining to the protection of personal data, but it regulates administrative issues, such as format and language of the document. Therefore, I will not discuss this Directive into more detail.

However, concerning to data quality issue as the impact of data matching in e-Audit, the issue of “accurate” in article 6(1) Directive 95/46/EC, in my view must be accompanied by article 12 of Directive 95/46/EC, pertaining to “right of data subject” to access their personal data.

Additionally, it is important to note, that the success of this Directive is not only because it involves official adequacy findings, but also due to its extra-territorial mechanisms. Article 25 (1) of Directive 95/46/EC states:

“The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions of this Directive, the third country in question ensures an adequate level of protection.”

Further, article 26 (1) and (2) provide exceptions to this main rule: (1) consent from data subject; (2) performing of a contract, (3) legally required on important public interest grounds, (4) protect the vital interests of data subject, (5) transfer is made from a register which according to laws and regulations is intended to provide information to the public or by a person who can demonstrate legitimate interests; and (6) the controller adduces

---

adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights.249

My point here is to describe the strictness of the EU mechanism in the case of transferring personal data of its citizen to third countries. It means that any country that wants to cooperate with the EU in ways that require personal data (such as trading) must meet the privacy standards set by the EU.

“"The PNR case”250 is an example of a case involving the transfer of personal data to third countries. Actually, the main discussion in this case is “proportionality issues” in order to measure the necessity of sending passengers’ data to the USA. However, this case provides insight into how the EU deals seriously with such matters in order to protect its citizens’ personal data, by prescribing that the US Bureau of Customs and Border Protection (CBP) must fulfil a sufficient level of protection for personal data transferred from the EU to the USA through an agreement dated 17 May 2004 between the European Community and the United States of America.251

Based on the above explanations, we can see how the EU protects the dignity, respect and integrity of its people through creating and implementing a clear and comprehensive mechanism. In addition, we can say that Directive 95/46/EC is a complete and comprehensive mechanism in processing personal data, compared to the Indonesian legal framework.

The responsiveness of directive of data protection in the EU to technical developments is more visible in the near future, since the EU introduced a new principle for the proposed regulation of data protection: “Privacy by Design.”252 Privacy by design means that “ICTs are designed and developed taking into account privacy and data protection.”253

To finish this discussion, as I stated before, I will present a European case in order to argue that even though public bodies have legitimate grounds for processing personal data, certain limitations still must be obeyed. In the 2003 case of Österreichischer Rundfunk (ÖRF),254 it was stated that the Austrian national measures regarding the duty of public institutions to inform auditors about salaries and pensions paid above a certain limit,

249Ibid.
250The PNR case is a case pertaining to the US rule to oblige European airlines flying to the US must provide the US custom authorities with the passenger name records, not only name and address of the passengers, but also contact details, such as: telephone numbers, e-mail address, credit card numbers, and meal ordered for the flight. Serge Gutwirth, et al., Reinventing Data Protection? <Netherlands: Springer, 2009> 33-34.
251Ibid., 34-37.
including the names of the present and retired employees who were recipients, are incompatible with article 8 of the ECHR and do not comply with the proportionality requirement in the general data protection directive.\(^\text{255}\) That information would be processed for annual reports which would be reported publicly with the objective of ensuring that public funds were managed well.

The European Court of Justice (ECJ) did some tests in this case, such as a “legitimate aim” and a “proportionality” test. They decided that even though the legitimate aim fulfilled article 8 (2) of the ECHR, the “proportionality” test failed.\(^\text{256}\) According to the court, “the communication of such data to third parties, in the present case a public authority, infringes the right of the person concerned to respect for private life, whatever the subsequent use of the information thus communicated, and constitutes an interference within the meaning of article 8 of the convention.”\(^\text{257}\) Further, paragraph 94 of the case claims that countries could determine, if sufficiently substantiated, that such disclosure is necessary for and appropriate to the objective of proper management of public funds.

The ECJ remarked on points in this case:

“The authorities and courts of the member states must not only interpret their national law in a manner consistent with The General Directive, they must also interpret The General Directive such that no conflict arises between the interpretation on which they rely and the basic rights protected by the community legal order or other general principles of community law such as the principle of proportionality.”\(^\text{258}\)

My concern in this part is to describe there is a different circumstance between Österreichischer Rundfunk case and the disclosure of the result of data matching system in e-Audit through the audit report.

In Österreichischer Rundfunk case, the disclosure of personal data (names and the amount of salary and pension) to the public is done merely to disclose personal information for the reason of transparency in accountability of public funds without any implication. I agree that there is privacy infringement in Österreichischer Rundfunk case, but it is under a legitimate ground.

However, in the case of the disclosure of personal data as the result of data matching system in an audit report, even for the reason of transparency, may often involve the suggestion that the data owner has committed fraud in management of state finances. In other words, when the public reads the report they will widely discuss data pertaining to the

\(^{255}\) Tranberg, 3.

\(^{256}\) Ibid., 2-3.

\(^{257}\) Joined Cases C-465/00, C-138/01, and C-139/01 Österreichischer Rundfunk (2003).

\(^{258}\) Tranberg, 3.
data owner. Moreover, the power of the recommendations of an audit report may lead to public’s assumption that the data owner is a corruptor.

It is important to go back to the duty of the Audit Board. Based on The 1945 Constitution, the Audit Board is an audit finance institution that functions to audit financial management and accountability of public finances. The only legitimate institution to judge a person guilty or not is the court.

Thus, I believe that to uphold the presumption of innocence principle in a democratic society, a suspect’s identity should not be disclosed in an audit report but only reported in a truly anonymous way. However, for the purpose of law enforcement, anonymity is absolutely excluded. After all, the Audit Board must explicitly mention personal data of the suspect by handing over the audit data (worksheets) to the law enforcement agencies for legal proceedings. Therefore, my point here is to underline that the principle of “notice” and “access and correctness” must be truly enforced before the audit report is submitted for the purpose of law enforcement.

As I already mentioned, after obtaining personal profiles as a result of the data matching system and after analyzing the profiles, if the auditors find strong indications involving the suspect, the auditors must promptly inform the suspect and give him an opportunity of accessing and correcting his personal data.

This is all the more important, considering the threats to privacy that might occur in every step of data matching system, which may result in inaccuracy and invalidity of personal data that supports an audit report.

4.4 Conclusion

Basically, the recognition of human rights in Indonesia legal system has been reflected in The 1945 Constitution and Pancasila as the philosophy of life of the Indonesian people. It means, privacy as part of human rights has been recognized in the Indonesian society.

However, the regulation of privacy and data protection in Indonesia has been organised separately and not comprehensively within the Indonesian legal framework as with the laws on banking, telecommunications, and criminal procedure.

This has occurred because the way in which Indonesian people interpret privacy differs from the interpretation of other countries. Although the basic concept of privacy as part of human rights is applied universally, but the type of communal society, the fact that information technology has not been applied as widely as in the developed countries, limited experience of privacy cases are factors that influence Indonesian people to interpret privacy. However, I believe that the involvement of Indonesia as part of global community and the invasion of information technology will inevitably result in a gradual demand that Indonesia alters its interpretation of the concept of privacy.
The democratic environment of Indonesia prescribes that Indonesian citizens participate in government activities by handing over their personal data. Nevertheless, the utilization of personal data among public bodies does not mean that personal data can be processed excessively. There should be a clear and comprehensive mechanism in place in order to safeguard the personal data of data owners.

Unfortunately, at present Indonesia only has Law Number 14 Year 2008, article 26 (1) and Law Number 14 Year 2008, article 17 (h) for regulating “consent” and kinds of personal data that cannot be disclosed publicly. In fact, the field of privacy and data protection is not only limited to the scope of those articles. As I previously mentioned in chapter 1, handling personal information is not a trivial issue.

In the case of the data matching system of e-Audit, in my view, the automatic processing of personal data will increase both the speed and the amount of personal data that are processed by the Audit Board. Therefore, an adequate safeguard for data owners is required, so the data owners can enforce their rights by controlling the flow of their personal information.

This requires the adoption of some existing international standards into the Indonesian legal framework, particularly those relating to data quality. The OECD and APEC have developed a considerable number of principles in the field of privacy and the transborder flow of personal data. Indonesia is as a member of APEC and has ratified the OECD guideline on the protection of privacy and the transborder flow of personal data. Indonesia should therefore consider adopting such principles as “notice”, “collection limitation”, “use limitation”, “data quality”, and “access and corrections”. However, these principles are also covered by the EU Directive on Data Protection, in addition to the fact that, as explained above, at present the EU Directive on Data Protection has proved to be the most accommodating directive not only within the EU, but also outside the EU, e.g., in Malaysia.

To sum up this section, learning from the Österreichischer Rundfunk (ÖRF) case, we can see that there are legitimate grounds for limiting the liberty of public bodies to access personal data excessively for reasons of transparency. Moreover, in the case of data matching in e-Audit, the publication of an audit report may lead to a corruption case.
CHAPTER 5—Conclusion and Recommendations

5.1 Introduction

This chapter summarizes the main points in order to provide answers to the sub-question of this thesis. The summary then provides a comprehensive conclusion to answer the main research question. Finally, recommendations for improving the remaining problems are presented.

5.2 Conclusion

Chapter 2

In conclusion, the Audit Board developed the data matching system in e-Audit in 2009 in order to accelerate good governance in Indonesia in the field of monitoring state finances. By using the “IPO model” approach, the data matching system can be divided into three phases: input, process, and output. During the input phase, the existence of the ETL process is required. Meanwhile for the matching process itself, the existence of the algorithms plays an important role in identifying “hits” in order to provide complete and comprehensive personal profiles. The data matching system is operated in BPK’s data centre and supported by components in BPK’s data centre: BPK data service, data quality management and data warehouse. These components have interrelationships with one another in order to support the matching system. However, the consolidator agent and the master consolidator agent are two applications that contribute a great deal during the pre-phase of the matching system.

Chapter 3

By using the “IPO model approach,” the following threats have been identified: during the input phase, re-using personal data may have an impact that it prevents data owners from controlling the flow of their personal information. In the process phase, the computer system impacts by reducing the involvement of human beings in analysing personal data. Hence, the auditor’s judgements on personal data, may become a threat during output, because it could cause auditors to rely too much on the profiles or to assess personal profiles excessively. Data quality and the excessive exposure of personal information in an audit report are the main issues in implementing the data matching system in e-Audit. I have shown that every phase of the matching system involves possible threats to privacy.

Chapter 4

As mentioned previously, the concept of privacy already existed in the 1945 Constitution, but comprehensive and clear regulations pertaining to privacy and data protection are still absent in the Indonesian legal framework.
The misinterpretation of the concept of privacy by the Indonesian people generates the perception that privacy is not part of human rights in need of protection. In the meantime, the lack of experience of the Indonesian people with privacy cases could result in the existence of the abstract concept of privacy being considered unimportant.

Nowadays, all countries in the world cannot deny the role of the development of information technology in supporting the prosperity of people. At present, it is necessary to enhance the information system in order to exist in the information age, specifically to support e-commerce on an international level.

We can see that Asian countries, such as Malaysia and the Philippines, already have a specific regulation on privacy data protection. In 2012, Singapore will follow Malaysia and the Philippines.\(^{259}\) I believe that even though Indonesia has a strategic place, geographically speaking, for international trading, that if this is not accompanied by a clear and comprehensive legal framework in the field of privacy and data protection, it will be difficult to become part of international trade.

Another reason that should be considered is the development of e-government in Indonesia, such as e-banking, e-learning and e-Audit which have been developed in order to support the implementation of good governance in Indonesia.

E-Audit has been developed by the Audit Board in order to strengthen the monitoring over public finances, considering the high level of corruption in Indonesia. One of the features provided by e-Audit is the data matching system which facilitates the analysis of personal data that are interconnected. However, based on my identification in chapter 3, every phase of this matching system may represent a threat in the privacy sphere.

Therefore, although the existence of OECD principles is accepted on an international level, adopting some related principles from the EU Directive on Data Protection would be the most adequate standard for dealing with the development of information technology. The adoption of such principles as “notice”, “collection limitation”, “use limitation”, “data quality”, and “access and corrections” should be considered. In addition, Indonesia can also learn from this directive how the EU regulates personal data transfer among countries.

In addition, in the proposed of The EU Data Protection regulation, the principle of privacy by design will be considered. This means that new technologies must be designed as “privacy friendly” in order to avoid threats that might arise with them. I believe this new principle will make the protection of personal data within the EU even more powerful, because the setting of privacy will be implemented since the design of a new technology.

---

\(^{259}\)Greenleaf, ASEAN’s ‘New’ Data Privacy Law: Malaysia, The Phillipines and Singapore, 4.
Conclusion

How Indonesian people interpret the concept of privacy influences the design of the existing Indonesian legal framework in the field of privacy and data protection. In addition, at present, Indonesia has not had a specific regulation in the area of privacy and data protection.

With regard to the implementation of e-Audit through data matching system, the absence of notification to data owners is the main problem that may cause the threat to privacy violation through data quality. Unfortunately, the existence of Law Number 14 Year 2008, article 26 (1) and Law Number 14 Year 2008, article 17 (h) that regulates “consent” and kinds of personal data than can not be disclosed to public are not adequate to respond to the main issue.

However, I believe, the demand for economic growth through international trading and the implementation of e-government in Indonesia will urge Indonesia gradually to design a clear and comprehensive legal framework in the area of privacy and data protection.

5.3 Recommendations

Based on the above main conclusion, I recommend:

1. The Indonesia government designs a complete and comprehensive legal framework pertaining to privacy and data protection gradually and based on the existing international standards. This legal framework will be useful not only for protecting privacy as a fundamental right, but also to accommodate the trend of e-government and the existence of Indonesia as a global community, as well. For the time being, “notice”, “collection limitation”, “use limitation”, “data quality”, and “access and correctness” principles may become the priority principles in order to enforce the data owners’ rights on their personal data. Besides, these principles may give a chance to the data owners to correct their personal information.

2. With regard to the implementation of data matching system in the context of e-Audit, the Audit Board should design a particular standard operational procedure for the matching system, regarding the types of personal data that will be matched and how details data set that will be designed, should be adapted with the kinds of audit that will be performed. In addition, due to the absence of a complete and comprehensive legal framework in the area of privacy and data protection in Indonesia, the Audit Board should adopt principles similar to those of Directive 95/46/EC into the Audit Board’s standard operational procedure for the data matching system, particularly in relation to the data quality principle. Some important points that should be covered in the standard operating procedure are: (1) anonymity in disclosing personal data into the audit report. It seems to me anonymity is the most adequate element that can support transparency issue without violating privacy; (2) there should be specific criteria concerning which
types of personal data must be matched. I mean, the matching process is only to be applied to the profile of the suspect from which there is already strong indication of corruption or fraud; and (3) finally, informing the data owners at the last phase of the data matching system will support the accuracy and the validity of the audit report and also give chances to the data owners to enforce their rights on their personal data.

3. As a preventive effort, the Audit Board could adopt the approach of “privacy by design” into e-Audit. I believe, during the development of e-Audit is not only limited for the matching purpose. Remembering, there is no differences of the life cycle between traditional audit and e-Audit. Therefore, it is possible that in the future the Audit Board will design e-Audit as a system, since planning phase until reporting. Here, the application of “privacy by design” should be applied into the system.

In the meantime, as a system e-Audit also will be improved through human resources. Improving the awareness of the auditors regarding the importance of privacy will be useful to prevent the utilization of the auditors’ judgement excessively. In addition, it will improve the abilities of the auditors to formulate the audit findings that are “friendly to privacy”.
BIBLIOGRAPHY

Books


Articles and Journals


**Internet publications**


**Case Law**


Joined Cases C-465/00, C-138/01, and C-139/01 Österreichischer Rundfunk (2003).

**Conference documents**


**Interviews**


**Legislations and other authoritative sources:**

(1) **General**


(2) **The EU legal framework**

Directive95/46/EC, On The Protection of Individuals With Regard to The Processing of Personal Data and On The Free Movement of Such Data.

(3) The Indonesian legal framework

Undang-undang Dasar 1945 (The 1945 Constitution)

Undang-undang Nomor 8 Tahun 1981 tentang KUHAP (Law of The Republic of Indonesia, Number 8 Year 1981 concerning Criminal Procedure).

Undang-undang Nomor 10 Tahun 1998 tentang Perbankan (Law of The Republic of Indonesia, Number 10 Year 1998 concerning Banking).

Undang-undang Nomor 36 Tahun 1999 tentang Telekomunikasi (Law of The Republic of Indonesia, Number 36 Year 1999 concerning Telecommunication).

Undang-undang 39 Nomor 1999 tentang Hak Asasi Manusia (Law of The Republic of Indonesia, Number 39 Year 1999 concerning Human Rights).


Undang-undang 15 Tahun 2006 <Law of The Republic of Indonesia, Number 15 Year 2006 concerning the Audit Board>.

Undang undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Law of The Republic of Indonesia, Number 11 Year 2008 concerning Electronic Information and Transactions).

Undang-undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (Law of The Republic of Indonesia, Number 14 Year 2008 concerning The Disclosure of Public Information).

Peraturan BPK RI Nomor 01 Tahun 2007 tentang Standar Pemeriksaan Keuangan Negara (the Audit Board Regulation Number 01 Year 2007 concerning Standard of Auditing of Public Finances).

Policy documents

Indonesia, BPK RI, Konfigurasi dan Mekanisme Aplikasi Konsolidasi Data.
Indonesia, BPK RI, Laporan implementasi e-Audit 2011 (Jakarta:2012).
Indonesia, BPK RI, Grand Desain e-Audit Menuju BPK Sinergi (Jakarta:2012).
Indonesia, BPK RI, Panduan Manajemen Pemeriksaan (Jakarta: 2008).

Indonesia, BPK RI, Strategic Plan 2011-2015 (Jakarta:2010).


Researchs
