Developing a Structured Metric to Measure Privacy Risk in Privacy Impact Assessments

Sushant Agarwal

Developing a Structured Metric to Measure Privacy Risk in Privacy Impact Assessments

Sushant Agarwal[1]

[1] Vienna University of Economics and Business, Institute for Management Information Systems, Vienna, Austria

Abstract. Today's IT applications involving the processing of personal data of customers are becoming increasingly complex. This complexity drives the probability of privacy breaches. Considerable damage to a company's reputation and financial standing may ensue. Privacy Impact Assessments (PIAs) aim to systematically approach and reduce privacy risks caused by IT applications. Data protection authorities and the European Commission promote using PIAs in application design to help attaining 'privacy by design' right from the inception of a new IT application. To help companies developing IT applications with conducting PIAs, many open-source tools are available online (GS1 tool, iPIA tool, SPIA tool etc.). Although these tools are modular and well structured, they fail to provide a metric to comparing progress in the implementation of privacy controls. In general, most of the tools use qualitative scoring for privacy risk, through which the measurement of progress is difficult. To address these shortcomings of existing tools, this paper presents a structured scoring methodology for privacy risk. A three-step semi-quantitative approach is used to calculate a relative score, which enables the comparison of privacy risks between incremental versions of an IT application. This comparison enables the monitoring of progress and thus, makes PIAs more relevant for the companies.

Keywords: Privacy risk, risk score, privacy impact assessment

1 Introduction

Privacy risk is defined as the risk of harm originating through an intrusion into privacy [1]. Not only can privacy breaches lead to lawsuits damaging a company's reputation and finances, but also can hamper trust of customers and overall brand perception. A PIA enables a company to identify risks pertaining to privacy and helps in adhering to data protection laws. Privacy Impact Assessments (PIAs) are crucial for companies using IT applications that process personal data of customers and employees. The European Commission acknowledges importance of PIAs and the proposed data protection regulations mandate PIAs where sensitive data is processed [2]. Also, a lot of tools have been developed to conduct PIAs such as - GS1 tool [3], iPIA tool [4], SPIA tool [5] etc. to support and ease the process of these assessments.

Literature emphasizes that PIA should be considered as a continuous process, so that engineers and managers of a company can consider the possible privacy issues through the complete IT development lifecycle to minimize the privacy risk[6, 7]. In most PIA reports, PIA results / outcomes are descriptive and long [8]. If PIA is to be considered as a continuous process then it's important to have a metric for comparison over time.

Progress in terms of privacy risks should be easy to measure and monitor using PIA, which is currently difficult.

Though, in the field of security risk management, extensive research has been done to quantify risk. Many methodologies have been proposed to define a numeric risk metric: probability models [9], decision-tree models [10], and composite indices based on impact and likelihood [11, 12]. These models stand in sharp contrast to the qualitative definition of privacy risk in most PIA methodologies [3–5]. For example, even though GS1 has a predefined number for the risk based on likelihood and impact and also a user selectable score for control effectiveness, the end score is still qualitative [3]. In UK's ICO code of practice for conducting PIAs, a template has been proposed which lacks a metric to score the privacy risks or to measure the improvements [1]. Oetzel and Spiekermann (2013) consider qualitative metric - low, medium, high for scoring privacy risk in the proposed iPIA tool [4]. Though the process is modular and captures both customer's and company's point of view, score is unstructured and difficult to measure. Also the EU CEN standards for RFID PIAs focus on qualitative evaluation of threats based on financial factors [13]. Hence, as far as to my knowledge, a metric to provide guidance to score a PIA in measureable terms has not been provided in the current literature so far.

To fill this gap, this paper proposes a structured privacy score metric for the PIA process. In the field of risk management, two approaches are mainly used to compute the level of risk. On one hand, the qualitative approach considers assets, vulnerabilities and threats to estimate an approximate risk level (generally as low, medium or high) [15, 16]. On the other hand, the quantitative approach considers risk score numerically as the product of likelihood and impact [11]. Qualitative scoring is used when the level of risk is low and it's difficult to quantify risks. In contrast, quantitative scoring is used when ample information about risk is available and likelihood and impact can be quantified [17]. However, privacy risk levels can be high but at the same time it is difficult to quantify impact and likelihood [18]. Therefore, a semi-quantitative approach is considered for this paper as it combines both qualitative and quantitative approaches to estimate the risk score. Using this approach a relative risk scale is defined to represent the severity [19]. As the risk score obtained is relative, this cannot be used to compare two different applications. But, can be used to compare the different versions of the risk assessment for the same application. This semi-quantitative metric enables companies to better monitoring and tracking of privacy risks throughout a system's development lifecycle.

The remaining paper proceeds as follows: in section 2, existing PIA methodologies are briefly described Section 3 proposes a new 3-step process of risk identification, modeling and quantitative evaluation. Section 4 illustrates the proposed methodology with a case study. Section 5 draws conclusions.

2 Current Practices for Privacy Risk

In the literature, many different methodologies [1, 4] and tools [3, 5] have been discussed (a good overview and evaluation of tools can be found in a paper by Wadhwa et al [14]). Three PIA tools are discussed here focusing on their methodology for scoring privacy risk.

2.1 GS1 PIA Tool

To 'rapidly perform a comprehensive assessment of privacy risks of any new EPC/RFID implementation' [3], the not-for-profit organization GS1 developed an easy to use MS Excel based PIA tool focusing on RFID implementation. For privacy risk, the tool has predefined levels of likelihood and impact and allows variable scoring for the control effectiveness. Even though scores for likelihood and impact can be changed, the main emphasis is on the control effectiveness score (level of maturity of implemented control to tackle privacy risk). Table 1 shows the scoring logic and each variable is scored on a scale of 1-5. Based on the level of PIA required, there are 5 risk areas with a total of 5 questions each for controls. While likelihood and impact are scored for a risk area, control effectiveness is scored individually for each control (C1, C2, C3, C4, and C5). Risk score follows a semi-quantitative approach and is measured based on the following formula 1:

$$Risk = Impact \times Likelihood - (C1 + C2 + C3 + C4 + C5) \qquad (1)$$

The methodology aims well at a numerical score to measure and monitor the privacy risks level. Also, scoring considers perspectives of both the data subject (usually the customer) and the organization (company). However, the criteria for scoring is broad and generalized i.e. not specific for privacy risks. For example, consider the following risk area – 'The data subject is unaware of the collection of personal data'. Criteria can be refined and narrowed down based on sensitivity, financial value of personal data for instance, to score the impact and likelihood for privacy risk score.

Score	Likelihood
5	It is very likely that this risk will occur in the organization
4	It is likely that this risk will

Score	Impact
5	The impact to the data subject will be highly detrimental and cause residual effects to the organization.
4	The impact to the data subject

Score	Control effectiveness
5	Risk mitigation strategy or control process in place - proven highly effective in the previous 12 months
4	Risk mitigation strategy or control process in

	occur in the organization		will be detrimental and cause residual effects to the organization.		place - proven effective in the past 6 months
3	This risk may occur in the organization	3	The impact to the data subject will be minor and cause some residual effects to the organization.	3	Risk mitigation strategy or control process in place - proven largely effective
2	It is unlikely that this risk will occur	2	There could be minor impact to the data subject with some residual effects to the organization.	2	Risk mitigation strategy or control process recently implemented - effectiveness is questionable or unknown
1	It is very unlikely that this risk will occur	1	There would be no impact to the data subject with no residual effects to the organization.	1	Risk mitigation strategy or control process is not in place or is under development

Table 1: Scoring technique used in GS1 PIA Tool

2.2 iPIA Tool

This tool has been developed at Institute for Management Information Systems, Vienna University [4]. It is an open source application written in PHP and JavaScript using jQuery UI. Similar to the GS1 tool, this tool also focuses on RFID applications. The process of assessment consists of 8 main parts and unlike other PIA tools, risk is not measured using impact and likelihood. Here, the degree of protection for each target is evaluated based on three demand categories: low, scored at 1; medium scored at 2; and high, scored 3. For this degree of protection there are two main dimensions split further into sub-categories. Based on this privacy target score, threats are then ranked in the subsequent steps. Table 2 shows the categories for the degree of protection for privacy target.

Instead of measuring the level of risk, this tool measures the level of protection required. The scoring is discrete and there is no overall score which makes it difficult to compare two different versions of a PIA report.

Category	Subcategory	Score
Operator perspective	Impact on reputation and brand value	Low, Med, High
	Financial loss	
Consumer perspective	Social standing	
	Financial well being	
	Personal freedom	
Overall category		

Table 2: Scoring technique used in iPIA Tool

2.3 SPIA Tool

Focused on both security and privacy, this tool has been developed by University of Pennsylvania [5]. Similar to GS1 tool this tool is also based on MS Excel spreadsheet. The tool has two risk scores for the pre-defined threat scenarios – 1) current state and 2) future state. For both these states, level of probability and consequence are entered and risk score is calculated as the product of probability and consequence. Table 3 shows the categories for probability and consequence.

Score	Probability
0	Threat does not apply to this application / database
1	The event would only occur under exceptional circumstances
2	The event could occur at some time, but probably will not
3	The event should occur at some time

Score	Consequence
0	Threat is not applicable to this application
1	Negligible impact on ability to plan and conduct business activities with minimal reduction in customer service, operational efficiency and staff morale. Very limited, or no financial/political impact
2	Minor impact on ability to plan and conduct business activities with minimal reduction in customer service, operational efficiency and staff morale. Minimal financial or political impact.
3	Medium impact on ability to plan and conduct business activities with a moderate reduction in customer service, operational efficiency and staff morale. Some financial or political impact is experienced.

4	The event will probably occur at some time	4	Major impact on ability to plan and conduct business activities with significant reduction in customer service, operational efficiency and staff morale. Considerable financial or political impact
5	The event is expected to occur in most circumstances	5	Comprehensive impact on ability to plan and conduct business activities with total disruption in customer service, operational efficiency and staff morale. Devastating financial or political impact

Table 3: Scoring technique in SPIA tool

This tool has a larger scale as compared to other tools but scores are still ambiguous as it is difficult to objectify difference between the different levels. For instance, the probability as "(3) should occur at some time" and "(4) probably occur at some time" are quite similar. Also, scoring for consequences is highly influenced by security risk assessment making it difficult to gauge the privacy risk.

2.4 Summary

It can be concluded, based on these tools (summarized in table 4), that scoring of privacy risks has not been well focused. The concept for scoring privacy risk has been adapted from IT security management literature [11]. This makes it difficult to score and increasing the ambiguity in the scoring. In other words, as the scoring criteria are generalized and not specific for privacy risk, it becomes difficult to assign a particular score for a privacy risk scenario. For example, likelihood is only based on the probability levels and lacks any criteria which changes the probability of a privacy breach like financial value, sensitivity of data, level of security of data etc.

Tool	**Pros**	**Cons**
GS1 Tool	Uses a semi-quantitative approach, considers control effectiveness to monitor the progress	Criteria for scoring is too generic
iPIA Tool	Considers operator and customer perspective separately	No risk score, protection demand is qualitative
SPIA Tool	Considers current and future state, aiming towards estimating the progress	Highly influenced by security risk assessment and scoring criteria are difficult to distinguish

Table 4: Pros and cons of the tools

3 A Proposed Methodology for Measuring Privacy Risk

The process of the proposed privacy risk scoring methodology involves three steps – 1) Risk Identification, 2) Risk Modeling (qualitative part) and 3) Risk Evaluation (quantitative part). First, in risk identification, scenarios for which risk is to be evaluated are considered. Second, in risk modeling step, qualitative modeling of the risk scenario is done so as to establish a relation between assets, vulnerabilities and threats. Third, in the risk evaluation step, a relative numerical score for the risk scenario is evaluated.

3.1 Risk Identification

This step involves identifying risk scenarios for the considered IT application. In this paper, risk scenarios are identified based on the EU data protection directive 95/46/EC [20] but can also be extended depending on the complexity of the application. These legal regulations also reflect company's perspective as following these regulations is one of the major considerations before deploying a new application. Risk scenarios are thus, the opposite cases of legal regulations as risk involved is doing something against the law. For instance, if the law states that the data should be used only for specified purpose, risk scenario would be - data is used for unspecified purpose i.e., worst-case scenario against a particular regulation (opposite of the regulation).

3.2 Risk Modeling

To analyze and score privacy risk, it is important to have a clear picture of the risk scenario involved. Therefore, this step deals with modeling risk scenarios qualitatively, which are identified in the previous step. It helps in understanding the complex risk scenario through abstraction. Hence, for scenario abstraction and for simplifying the scenario, CORAS diagrams are used for modeling. CORAS approach is a general approach for risk analysis and fits well with privacy risk scenarios. Qualitatively, the risk is defined as the potential for loss, damage or destruction of an asset as a result of a threat exploiting vulnerability.. Figure 1 shows a generalized CORAS risk diagram. It starts with who all can expose the system to risk (which includes system design as well). Usually, the negligence of employees to handle the data properly or poor system design can lead to a privacy breach. Then, vulnerability, which is basically a weakness, is identified. This vulnerability can be exploited by a threat to depreciate the value of an asset. Then the threat corresponding to the vulnerability is determined which is simply the cause for unwanted incident. Similarly, unwanted incident is then classified which is the scenario when the vulnerability is exploited by the threat. Lastly, asset loss i.e. asset which is affected by the unwanted scenario is depicted in Figure 1.

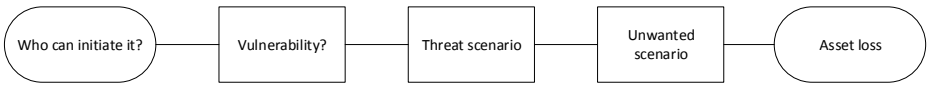

Figure 1: Schematic of risk modeling using CORAS approach

Figure 2 shows an example of CORAS diagram for EU directive 95/46/EC article 6 about personal data being processed fairly and lawfully [20]. If privacy concerns are undermined then there is less chance of fair and lawful processing. Negligence of employees, mischief of a hacker as well as poor system design can initiate the threat. Vulnerability here is, thus, ignoring / not considering the regulations. As a result, the threat is usage of personal data against the law leading to an unwanted incident as either lawsuit(s) against the company or bad publicity in the media.

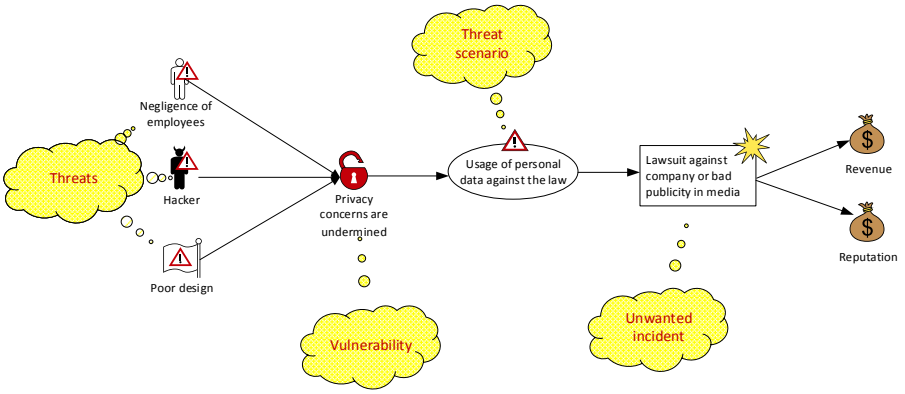

Figure 2: Example of risk modeling using CORAS approach

3.3 Risk Evaluation

After defining the risk qualitatively, this section attempts at quantification of risk score for the modeled scenario. Similar to the IT security risk management approach [11], privacy risk is defined as the product of impact and likelihood explained in the subsequent sub-sections.

Impact.

For assessing the impact Solove's taxonomy is used [21]. The taxonomy focuses on specific activities that may pose privacy problems rather than just the definitions of different aspects of privacy. Also it aims at activities that create privacy problems and that can upset the balance of social or institutional power in undesirable ways. This makes it easier to match and relate it to the risk diagrams. The taxonomy is split into four categories: 1) Information collection – related to collection of data, 2) Information processing – involves the way information is stored, manipulated and used, 3) Information dissemination – is about circulating and sharing the information, 4) Invasion –

involves interference into people's private affairs. These four categories are subsequently split into further categories. Table 5 shows the different dimensions based on Solove's work. Some principles are not considered because they are not relevant for the scope of privacy risk involving customer-company relationship. For instance 'interrogation', which is various forms of questioning or probing for information, is highly unlikely in this scenario. Also, 'decisional interference' is excluded as it's related to government's incursion into the data subject's decisions regarding his/her private affairs.

Category	Subcategory
Information Collection	Surveillance
Information processing	Aggregation
	Identification
	Insecurity
	Secondary Use
	Exclusion
Information Dissemination	Breach of confidentiality
	Disclosure
	Exposure
	Appropriation
	Distortion
	Increased Accessibility
Invasion	Intrusion

Table 5: Dimensions for impact based on Solove's taxonomy

Each risk scenario is considered and matched with different dimensions of impact. Then a simple sum of the categories applicable for the directive is calculated. This sum becomes the impact score for the risk scenario. For example, according to EU directive's article 6, collected data should be accurate. For this article, risk scenario would be the worst-case possibility i.e. very low data quality. Poor accuracy can lead to 'exclusion' as wrong information might devoid an individual from some offer [21, p. 521]. Similarly, it can also lead to 'breach of confidentiality' [21, p. 524]as an individual trusted the company and had high confidence while sharing personal data. It can also lead to 'distortion' [21, p. 546] as the personal information about the individual has low accuracy and wrong information would lead to distortion if used in some application. Therefore, three dimensions are valid for low data accuracy or low data quality. For scoring, simplistic harm benefit analysis is considered. All the different dimensions here are considered as harms and there are no benefits. So, the impact score is the net harm, which is the number of the affected dimensions, 3 in this example.

Likelihood.

For measuring likelihood, Lipton's work on 'Mapping online privacy' is used [22]. This work focuses on privacy issues related to digital data. Unlike Solove's work, giving the methodology a broader view by incorporating online privacy of customers. It identifies

6 different dimensions of privacy – 1) Actors and relationships includes all those involved in a privacy incursion, 2) Conduct is about privacy threatening activities, 3) Motivations is simply about the motives for privacy threatening activities, 4) Harms and remedies includes all the harms and ways to redress those harms, 5) Nature of information is about the content of the information and 6) Format of information, which is about the format used to gather information online and disseminate it later. To estimate likelihood four of the six dimensions (i.e., all except 'conduct' and 'harms & remedies' which are similar to privacy risk and its consequences respectively) are used to measure likelihood.

The dimensions of likelihood are broadly classified in two categories – 1) Actors involved and 2) Data Characteristics. The data characteristics category incorporate the different dimensions of motivation, nature and format of information. Figure 3 shows the different dimensions of likelihood. Actors involved can be divided into 3 categories – First, the company, which involves both the employees and system design (also a strong passive actor in relation to the personal data). Second, 3rd parties which are involved in handling the personal data and third, other actors like competitors and hackers who also have interest in the collected personal data of the customers. Similarly, data characteristics is also divided into 3 categories – 1) Amount of data, 2) Sensitivity of data, 3) Value of data involved. Amount of data is about the total rows and columns of the data. If more data is collected then the likelihood of privacy risk in general increases. Also, the value of data is about the monetary benefits of a privacy breach. If cost of an activity leading to privacy risk is low than the likelihood will be higher as vulnerability can be exploited easily without any substantial cost. Similar is the case with benefits obtained with that malicious activity, i.e., the higher the financial value of data, the higher is the likelihood of occurrence of similar activity. Additionally, a category regarding sensitivity of data is considered for measuring likelihood because financial value is not always higher for more sensitive data as it depends more on the context. For example, CEN standards define a higher asset value to an email address as compared to racial origin, which is actually a very sensitive data type. But, as maybe current scope of commercial exploitation is not that high for racial origin (as compared to email address), there is a higher commercial value for email addresses. Nevertheless, sensitive data is usually intimate for the customers and this gives a high motivation to the actors who have intentions of damaging the reputation of the firm collecting and disseminating the personal sensitive data.

4 A case study – Application to the law

In this section a case study is presented to illustrate the proposed methodology. A fictitious restaurant with an online ordering and home delivery system is considered for the example. Customers can open restaurant's webpage, order food, pay it online and can get it delivered to their desired address.

According to article 6 of EU data protection directive – 'personal data of data-subjects must be adequate, relevant and not excessive in relation to the purposes for which

they are collected and/or further processed'[20]. The risk scenario would therefore be collection of personal data inadequate, irrelevant and excessive for the purpose.

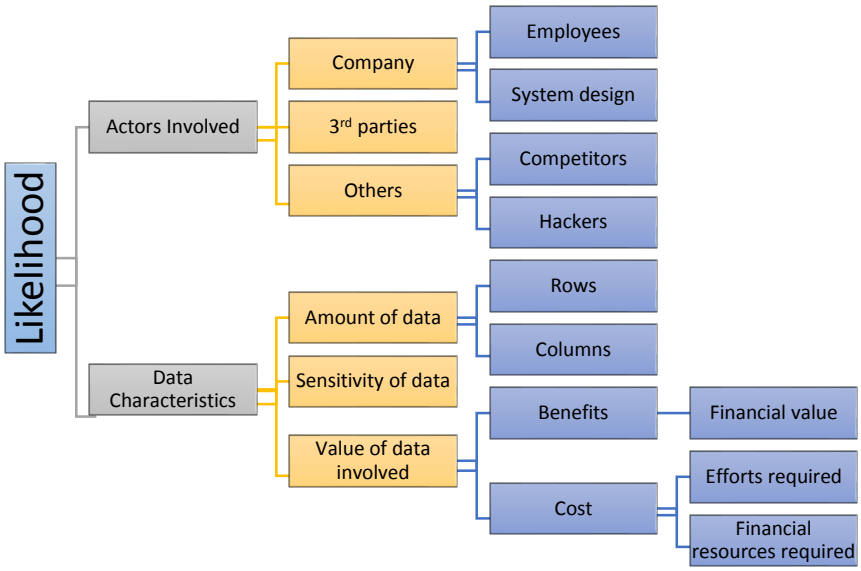

Figure 3: Dimensions for measuring likelihood

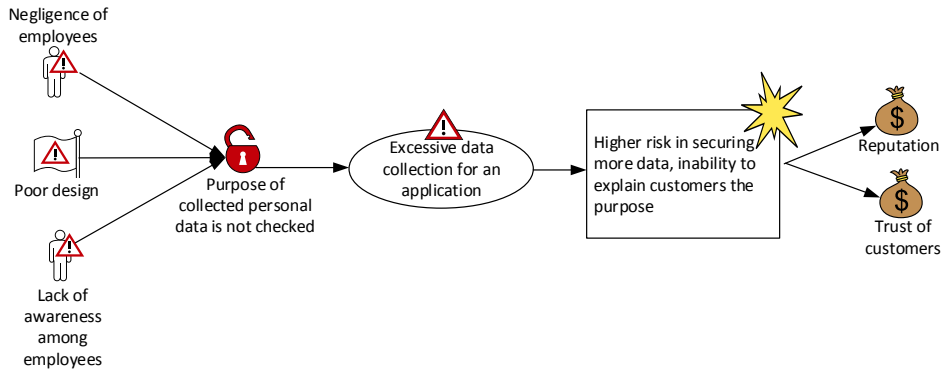

Figure 4: CORAS diagram for the risk scenario

Figure 4 shows the modeled risk diagram for the scenario. Due to either negligence of employees, their lack of awareness or the poor design of the system can lead to scenarios where data collected is excessive of the purpose. Underlying vulnerability here is that before deploying a system or during its design the purpose of collected personal data fields is not checked or actively updated with the changes in the design. This vulnerability is leads to a threat, which is simply the excessive data collection (opposite scenario of the legal regulation). Then, unwanted scenario for this threat would be higher risk in securing and handling more data fields as compared to the case when

limited data would have been collected. Also, according to article 10 of EU data protection directive [20], data subjects should be given the information regarding the purpose of data collection which would be difficult to provide as data collected is excessive to the purpose. Hence, it will lead to loss of reputation and trust of customers (data-subjects) for the company.

Let us assume that the restaurant collects the personal details as shown in table 6. The purpose is to process an online order and deliver the food at the given address which requires last name to identify a person, address to deliver it and telephone number to notify when the delivery staff is at the given address.

Category of personal data	Collected	Required for the purpose?
First name	Y	N
Last name	Y	Y
Address	Y	Y
Telephone	Y	Y
Email	Y	N
Gender	Y	N
Birthday	Y	N
Order history	Y	N
Browsing history	Y	N

Table 6: Categories of personal data collected by the restaurant

The next step is quantifying the impact and likelihood score. Using Solove's (2006) taxonomy, the impact dimensions are measured as shown in table 6. If excessive data is collected then it can lead to increased surveillance with the help of excessive data fields that are collected. In the example, browsing history is a case of surveillance on customer's browsing habits. Similarly, it also leads to aggregation as a more comprehensive profile of the customers would be collected, which can also lead to identification. In general, customer would be roughly identified for the delivery using last name and address but the data collected would lead to exact identification. Also, more data leads to more insecurity and might tempt the restaurant for other secondary uses like sending marketing emails based on customer profile. Personal data of a customer can be also misused by an employee or a hacker to use his/her identity for a malicious activity leading to appropriation. Company would have increased accessibility about the customer and would be in fact intruding in customer's personal life by collecting personal information, which is not required for the application. Therefore the impact score is quite high as 9/13.

The likelihood score would be subjective and more context dependent. For this scenario, the main actors are easily identifiable – system design and employees at the restaurant. Data characteristics score would depend on the quantity, financial value, and sensitivity of the collected data. Considering the fact that only the basic demographics

like name, age, address and phone numbers are collected, the score would be 2/3. For sensitivity it would be 0. For amount of data the score can be set to 1 (out of 3) as not much data is collected. Value of data would be around 2 out of 3 as address, telephone numbers, browsing history etc. have high marketing value. In total, the score for likelihood would be 5/10 as shown in table 8.

Dimensions for impact	S U M	**Surveillance**	**Aggregation**	**Identification**	**Insecurity**	**Secondary Use**	**Exclusion**	**Breach of confidentiality**	**Disclosure**	**Exposure**	**Appropriation**	**Distortion**	**Increased Accessibility**	**Intrusion**
Excessive collection	**9**	Y	Y	Y	Y	Y	N	N	Y	N	Y	N	Y	Y

Table 7: Impact score for the example

Dimensions	**Score**	**Max**
Actors involved	2	3
Amount of data	1	3
Sensitivity of data	0	1
Value of data	2	3
Total	**5**	**10**

Table 8: Estimating the likelihood

Hence, the risk score would be 8.75 out of 25 as shown in the table 9. The scale has been adjusted such that the maximum risk score would be 25. The risk is then represented on a an impact-likelihood (probability) graph [11]. It can be observed from the graph in figure 5 that risk score lies in the escape/transfer region. Hence, it is required to escape the scenario by modifying the design of the system, which can be either done by an audit to confirm the use of all the data collected or by reducing the personal data which is being collected. Subsequently, in the later stages, likelihood can be decreased by improving the system design or securing the collected data (to increase the efforts required for unreasonable access). Similarly, impact would be reduced when limited data is collected for a predefined purpose as dimensions of intrusion, surveillance etc. would then not be valid.

	Score	Score out of 5
Impact	9/13	3.5
Likelihood	5/10	2.5
Risk score		**8.75 / 25**

Table 9: Calculating the risk score

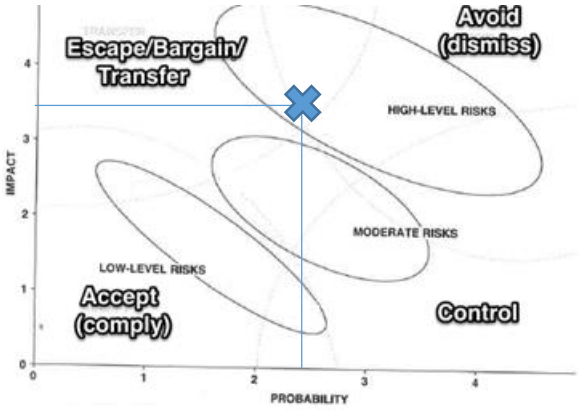

Figure 5: Risk score on impact likelihood graph

5 Conclusions and Future Work

Following an IT security risk management approach, this paper proposes a structured privacy risk metric. The risk score enables measuring the progress made in minimizing privacy risk between the incremental development cycles in system development. Risk scenarios based on EU data protection directive 95/46/EC have been taken as an example to illustrate the process. These scenarios are modeled using CORAS diagrams for better understanding and abstraction. For quantification, risk is then broken down into impact and likelihood. The dimensions for likelihood focus on company's perspective by considering actors, financial value of data etc. and dimensions for impact based on Solove's taxonomy help in measuring the impact from the customer's point of view. In the end, a privacy risk score is obtained as the product of impact and likelihood.

The focus in previous sections has been to develop a structured metric for privacy risk score and scales for measuring impact and likelihood are not discussed in detail. 0 and 1 have been used for scoring the impact dimensions and all of them have the same weightage. However, impact dimensions can have different weightages based on the scenario. For example, consider a scenario where CCTV cameras are used in a store for surveillance. If cameras are around the changing rooms then it can lead to 'Exposure' of customers i.e. might reveal their nude body. In this scenario, weightage for 'Exposure' should be higher than 'Aggregation' of their purchase history. Hence, the future work would involve selecting suitable functions to aggregate impact dimensions along with assigning appropriate weightages to them. Additionally, the scoring metric would then be integrated in a PIA tool to benchmark it in a real-life scenario. It would be crucial to tackle the tradeoff between customizability and complexity. A rigorous and

fully customizable risk scoring algorithm might lead a complex PIA process whereas, standardizing all the parameters might reduce the usefulness of the score. Hence, for a simple yet meaningful PIA, it is important that scoring process does not add a lot of complexity to the process.

6 References

1. Information Commissioner's Office UK: Conducting privacy impact assessments code of practice. 50 (2014).
2. European Commission: Proposal for protection of individuals with regard to the processing of personal data and on the free movement of such data. 0011, (2012).
3. GS1: GS1 EPC/RFID Privacy Impact Assessment Tool, (2012).
4. Oetzel, M.C., Spiekermann, S.: A systematic methodology for privacy impact assessments: a design science approach. Eur. J. Inf. Syst. 23, 126–150 (2013).
5. University of Pennsylvania: Introduction to the SPIA Program, http://www.upenn.edu/computing/security/spia/spia_step_by_step.pdf.
6. Spiekermann, S.: The RFID PIA – Developed by Industry, Endorsed by Regulators. In: Wright, D. and Hert, P. (eds.) Privacy Impact Assessment. pp. 323–346. Springer Netherlands (2012).
7. Wright, D., de Hert, P.: Privacy Impact Assessment. Springer (2012).
8. PIAw@tch: Significant Privacy Impact Assessment Report accessible online, http://www.piawatch.eu/pia-report.
9. Cheng, P.C., Rohatgi, P., Keser, C., Karger, P.A., Wagner, G.M., Reninger, A.S.: Fuzzy multi-level security: An experiment on quantified risk-adaptive access control. In: Security and Privacy, 2007. SP'07. IEEE Symposium on. pp. 222–230 (2007).
10. Sahinoglu, M.: Security meter: A practical decision-tree model to quantify risk. IEEE Secur. Priv. 3, 18–24 (2005).
11. Vose, D.: Risk Analysis: A Quantitative Guide. John Wiley & Sons (2008).
12. ISO: ISO/IEC 27005 Information technology - Security Techniques - Information security risk management. ISO/IEC (2008).
13. CEN: Information technology - RFID privacy impact assessment process. (2014).
14. Wadhwa, K., Rodrigues, R.: Evaluating privacy impact assessments. Innov. Eur. J. Soc. Sci. Res. 0, 1–20 (2013).
15. Yazar, Z.: A qualitative risk analysis and management tool--CRAMM. SANS InfoSec Read. Room White Pap. (2002).

16. Vellani, K.: Strategic Security Management: A Risk Assessment Guide for Decision Makers. Elsevier Science (2006).

17. Stoneburner, G., Goguen, A., Feringa, A.: Risk management guide for information technology systems. Nist Spec. Publ. 800, 800–830 (2002).

18. Data Security and Privacy Group Edelman: The costs, causes and consequences of privacy risk.

19. Borghesi, A., Gaudenzi, B.: Risk management: How to assess, transfer and communicate critical risks. Springer Science & Business Media (2012).

20. European Parliament: Directive 95/46/EC. Off. J. Eur. Communities. L 281/31, (1995).

21. Solove, D.: A taxonomy of privacy. Univ. PA. Law Rev. 154, 477–560 (2006).

22. Lipton, J.D.: MAPPING ONLINE PRIVACY. Northwest. Univ. Law Rev. 104, 477–515 (2010).