Towards Legal Privacy Risk Assessment Automation in Social Media

Ebenezer Paintsil and Lothar Fritsch

paintsil@nr.no, Lothar.Fritsch@nr.no

Abstract: End users activities in social media lead to regular changes in the overall privacy impact because they continually encounter or meddle in all forms of private data associations. Users are exposed to regular changes in risk level as a result of regular updates. To keep an overview over risk exposure, privacy risk assessments, in theory, should be re-done upon every update in a user's network. End users could reduce their risk assessment burden if they could rely on an appropriate risk assessment tool providing information on risk levels as a result of changes in associations. We have several information technology (IT) security risk assessment tools available for such purpose. However, we cannot rely on such tools for legal privacy risk assessment because of their classic security focus. The security-focused risk assessment tools are based on the knowledge of security experts, and have strong focus on tangible assets and system security. Using such security risk assessment tools to assess legal privacy risk may impair communication and understanding, and may increase uncertainty in the risk estimation because such tools lack the domain knowledge. A risk assessment tool base on the legal privacy principles can reduce uncertainty in the risk estimation and enhance the risk assessment communication. This article focuses on privacy risk assessment from a legal perspective and how it applies to social media.

1 Introduction

Social media allow two or more end users to interact using an online network. We have two main stakeholders in social media interactions - the service provider (SP) and the end users. The SP regulates the terms of use with a privacy policy, an access control policy or a contract between him and the end user which is usually static. However, end users interact with other end users with policies that may change regularly as depicted in Figure 1.

Figure 1 depicts a simple example of end user interactions in a social media. The End user 1 interacts with the End user 2 who in turn interacts with End user 3 and 4. When end users interact with each other, the system creates a particular access control or privacy policy to regulate the terms of use of their individual personal data. Also, the individuals may choose a particular policy to regulate the terms of use of their personal data. We label these policies as P1, P2 and P3. The policies P1, P2 and P3 may change regularly due to regular changes in individual preferences. They represent end users' privacy or access control policies. The regular privacy policy changes may lead to a privacy risk level unknown to the end user. In addition, it is impossible for the system owner to assess the privacy risk of the system as a whole. A tool that can support end users to understand

erschienen im Tagungsband der INFORMATIK 2011
Lecture Notes in Informatics, Band P192
ISBN 978-3-88579-286-4

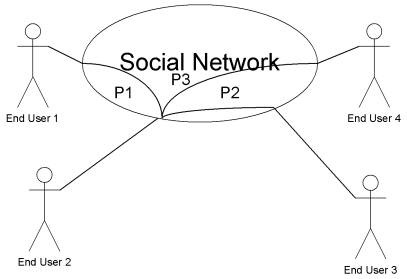

Figure 1: End User Interactions

their risk level as a result of an interaction would be appropriate for the individuals to manage their privacy risk.

However, such legal privacy risk assessment tool should not base on the traditional information technology (IT) risk assessment methods because they depend on the security risk assessors' experience [Ave08], [Wan05], and have strong focus on tangible assets and system security. The security-focused risk assessment methods may lead to ineffective communication strategies, high level of uncertainty in the risk estimation and incomprehensive risk estimation metrics. An example is the Risk IT framework's risk impact communication strategy. The Risk IT framework relies on the COBIT Information Criteria, Balanced Scorecard Criteria, COSO and Westerman techniques to communicate risk impact to stakeholders [ISA09]. However, these communication techniques are organization-focused because they express risk impact in business and financial terms.

The objective of this article is to explain the importance of legal norms in privacy risk assessment and how they distinguish IT security risk assessment from legal privacy risk assessments. Further, we introduce a conceptual model for legal privacy risk assessment leading to a proposal towards automation. We demonstrate a possible application of the proposal to privacy risk assessment of social media.

The rest of the article is organized as follows. Section 2 covers the related work in risk assessment. Section 3 is the requirements for legal risk assessment; section 4 covers legal risk modeling with CORAS risk assessment method. Section 5 is the legal risk specification, and a case study. Section 6 states the conclusion.

2 Related Work

Privacy Impact Assessment (PIA) is a framework for assessing the impact of personal data processing activity on privacy before an information system is implemented [Off09]. The PIA is a compliance check between personal data processing activities and privacy laws, policies, or regulations. It specifies a framework or requirements for privacy risk assessment without an explicit risk assessment technique or method. The PIA does not

focus on risk assessment automation. We focus on an explicit method or approach for legal privacy risk assessment and automation.

Security-focused approach to privacy requirements engineering is unsuitable for privacy risk assessment because of the overlapping nature of security and privacy [ANM09]. Abu-Nimeh and Mead propose security risk assessment along with PIA using the Security Quality Requirements Engineering (SQUARE) method [ANM09]. Mitrano, Kirby and Maltz in their presentation sought the need to incorporate private measures into security measures because they complement each other [TMM05]. They distinguished privacy risk assessment from security risk assessment by stating that security risk assessment concerns with physical asset protection and asset protection policies but privacy risk assessment focuses on data protection and data protection policies. However, the contributions of normative values to legal privacy risk assessment were not emphasized in both approaches.

Wang introduces the need for security metrics in [Wan05]. Security metrics help with risk assessment (RA) and security awareness within an organization. Wang suggests five requirements for security metrics including the quantitative metrics. Quantitative metrics reduce subjectivity and increase the level of trust. However, Aven disagrees with these assertions and argues that the arbitrariness in quantitative risk estimation "could be significant, due to the uncertainties in the estimates or as a result of the uncertainty assessments being strongly dependent on the assessors" [Ave08]. He suggests a mixed approach called semi-quantitative. This combines both quantitative and qualitative techniques. Its intention is the reduction of uncertainty. Nevertheless, Aven did not consider how the relationship between qualitative RA and the background of the risk assessor contribute to the uncertainty in the risk estimation. For example, a legal privacy risk assessment would require a lawyer as a member of the team. It would be inappropriate for the lawyer to estimate and communicate legal risk with quantitative or semi-quantitative values because legal risk depends on normative values instead of quantitative or semi-quantitative values.

Breaux et al. provide a systematic technique for analyzing, deriving and automating security requirements from regulations [BMAM08], [KZB+07]. They developed a requirements engineering methodology for extracting and automating stakeholder rights and obligations from regulations such as Health Insurance Portability and Accountability Act (HIPAA). These enable software engineers to reason about the requirements necessary to comply with the law. We consider these requirements as values that can be used to automate legal privacy risk assessments. In addition to right and obligation, we include legal competence normative values or requirements so that we can model legal privacy contracts.

3 Legal Risk Assessment, Privacy, and Social Media

Legal propositions or norms and "normative values" are central to legal risk assessment. We regard normative values as standards for assessing legal reasoning. They include obligation, permission, exception and right. We refer to them as legal modalities. Normative values may be referred to as norms [Bul92], [Sar06]. A legal norm consists of facts (legal

antecedents or something that must happen before) and consequences [VLM+05]. The antecedent describes which factual circumstances have to be present for a normative value to apply. The consequent indicates the legal implications of the applicable normative value. Thus, normative values may connect a legal antecedent to a legal consequent or determine the transition from legal antecedent to legal consequent.

Legal antecedent is either a fact or a proposition. A fact is something that is established to be true and may not be disputed. A proposition is something that is true, believed to be true, known to be true, ought to be true, eventually true or is necessarily true. We refer to the words "ought to, believe, known, eventually and necessary" as the modalities of the proposition.

We refer to legal modalities as normative values and categorize them as normative values for conduct, competence and right. The normative values for conduct (command) require a stakeholder to conditionally perform an action [KZB+07]. The competence normative values confer public or private power, immunity, subjection, disability etc. on a legal person [Bul92], [Sar06]. They may determine the validity of legal power or capacity. Legal competence may grant the capacity to create legal rules binding others or oneself. Legal right permits a stakeholder to conditionally perform an action that may advance his/her interest or the interest of others.

The normative values are obligation, permission, prohibition, commitment, rule, authority, power, right, responsibility, and exception [Enc10], [Sar06]. "Facultative" is a special kind of normative value which permits an action and its negation [Sar06]. Unlike traditional risk assessment, normative values may play an important role in legal risk assessment. Nevertheless, their thorough analysis and relationships are beyond the scope of this article. For more information on legal norms refer to [JS96],[Har94], [Bul92], [Sar06].

How we choose an applicable legal norm depends on the applicable law. The mandatory or regulatory character of the rules laid down in privacy law determines the applicable legal norm. Rules of mandatory law are generally rules from which the parties cannot derogate by contract [Edw05],[Cui07]. The right to withdraw from a contract, and protection against unfair contractual terms are mandatory rules.

Similarly, the applicable normative values for privacy risk depend on the nature of privacy law and regulation. Deciding the nature of an applicable privacy law is not a straightforward matter. It is, e.g., not clear that the nature of rules laid down in the European Union (EU) data protection directive (DPD) [Com95] is that of rules of mandatory law. Cuijper [Cui07] believes that the EU DPD does not require implementation into mandatory rules of law. The objectives focus on individual protection when processing and moving personal data. She emphasized the latter as more important. The regulation of free movement of personal data does not mandate the implementation of the DPD into mandatory rules of law. In addition, she stressed that the directive contains no clause requiring mandatory law and DPD article 7 [Com95] leaves room for processing of personal data based on contract. Cuijper concluded that, "it will be a step too far to denounce judicial effect to all contracts between data controllers and data subjects in which the data subject willingly gives up part of the rights granted to him on the basis of this directive".

However, Bergkamp argues otherwise. Here, the "DPD establishes a public law regime

ISBN 978-3-88579-286-4

that cannot be varied by a private law contract" [Ber03, p. 123]. Even Cuijper [Cui07] noted that the argument for private law regime depends on whether the data subject has a strong bargaining power. Where the data subject is the weaker party, the law may have to give the data subject a strong protection. In addition, the data controller may process personal data under the EU DPD without a contractual agreement [OM07]. The lack of legal consensus between the public and private law character of the DPD represents legal uncertainty that can contribute to legal privacy risk. Furthermore, the nature of the applicable privacy law is an important modality to consider in legal privacy risk assessment because it determines the applicable normative values.

In social media, however, the role distribution between data subject, data processor and data controller becomes more obfuscated. A user receiving an association becomes implicitly a data controller. A user creating new associations implicitly becomes data processor. This peer-to-peer, interdependant data processing regime distributes the policies for data use over many users, which all can alter their part of the policies and associations at any time. Recent literature points out, however, that users in social media can legally be treated as data controllers, according to European legislation [Par09],[Won09].

4 Legal Privacy Risk Assessment Conceptualization

Currently, there are over 200 risk management methods with no adequate selection criteria [MMM+08]. We selected the CORAS [MSL11] risk assessment method because it is a well-documented risk assessment method, has straightforward risk assessment concepts and attempts to model legal risk. CORAS manages risk in eight steps but the central concepts revolve around the combined effect of threat, vulnerability, threat scenario, unwanted incident on an asset [MSL11]. A threat exploits vulnerabilities in an asset, leading to a chain of events called threat scenario that may lead to unwanted incident that may in turn cause loss to a system owner or a stakeholder.

Figure 2 depicts a risk assessment conceptual model based on the CORAS risk assessment concepts. It also depicts one of the fundamental differences between legal risk assessment and information technology (IT) security risk assessment. Figure 2(a) represents a simple IT security risk assessment scenario and 2(b) is the legal risk assessment scenario. Quantitative values determine the transitions in Figure 2(a) reflecting a good security risk assessment [Wan05]. Nevertheless, the transitions in Figure 2(b) are determined by normative values (obligation and prohibition) reflecting legal decision-making. Legal decision-making depends on normative values rather than quantitative values.

Unlike IT security risk assessment, legal risk assessment relies on legal antecedents, normative values and legal consequents to determine the effect of a legal breach [VLM+05], [Mah10]. Therefore a risk assessment method based on quantitative values may not make legal sense. We determine the risk by measuring the extent by which the legal breach impact on the objectives of the system owner or a stakeholder. This is referred to as risk tolerance [ISA09]. We have security or privacy risk if the loss is higher than the acceptable risk level or risk tolerance. The risk tolerance and the decision to arrive at the loss should

ISBN 978-3-88579-286-4

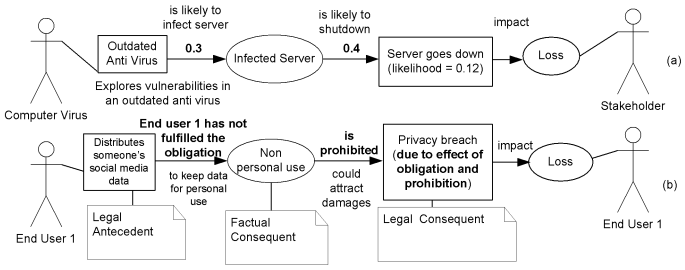

Figure 2: Diagram (a) Represents a Simple Security Risk Assessment Scenario and (b) is a Simple Legal Privacy Risk Assessment Scenario

be deduced from the legal rules and applicable case laws.

In Figure 2(b) a legal antecedent may lead to a factual consequence. Legal antecedents may consist of one or more facts that may lead to a factual consequent. The Legal Antecedent and Factual Consequent have both legal propositions and factual propositions. Similarly, the Legal Consequent has factual propositions and legal propositions.

This conceptualization highlights one of the possible ways of reasoning about legal privacy risk. The directed graph and the normative values could make it possible to use hybrid modal logics for the legal privacy risk specification leading to a possible automation. Consequently, we model legal privacy risk as a directed graph with normative values that determine the transitions leading to a loss.

5 Hybrid Language Specification

The expression such as "ought to, believe, known, eventually and necessary" are refered to as modalities. We use a modal expression such as ought to, believe, necessarily and possibly to qualify the truth of a judgment [Gar09]. Modal logic is the study of the deductive behavior of the expressions such as 'it is necessary that' and 'it is possible that'. Modal logic is highly expressive and suitable for directed graph [BvB88]. They provide a good balance between expressiveness and complexity. Most importantly modal logic is syntactically simple language and mathematically rich [PBV10, p. xii-x].

A directed graph or a relational structure is a set of nodes and some edges between them [BvB88]. It is defined as $\langle W, R\rangle$ where W is non-empty set of the vertices of the relational structure called the worlds. The members of W represent the states, points, nodes, times, instants or situations of the relational structure. The R is the set of edges of the relational structure representing the accessibility relation between worlds. The cross product $\{W \times W\}$ stands for $\{(w_1, w_2)|w_1 \in W, w_2 \in W\}$ the set of all ordered pairs (w_1, w_2) where w_1 and w_2 are from W. The set $R \subseteq W \times W$ is the binary or accessibility relation over W. A model in modal logic is a relational structure with valuation i.e. $M = (W, R, V)$ where V is the valuation. The valuation determines the truth or falsity of a proposition or

a formula.

Hybrid modal logic extends modal logic. In addition to the set of proposition at each world, hybrid modal logic introduces special propositional symbols known as nominal. A nominal is true at exactly one world of a model [BCT04]. Hence, we can use it to name a state. Further, hybrid modal logic introduces a state variable, an atomic formula denoting a state. It has additional operators such as @ and $\downarrow$ which are not found in modal logics. The $\downarrow$ is known as the binder. It is possible to express irreflexivity of a state with the binder. Using $\downarrow$ allows one to name a world where a formula such as $\downarrow x\Psi$ is evaluated. The x is a state variable or a nominal and Ψ is a formula. $\downarrow x\Psi$ binds all the occurrences of x in Ψ to the current state, thus the state where evaluation is occurring [BCT04]. The @ operator allows us to "jump" to another world or a state in a frame to evaluate a formula. For example, the formula $@_x\Psi$ is true if Ψ is true at the world denoted by x.

Another important aspect of modal logics is their ability to express modalities. The basic modalities are necessarily and possibly. The necessarily is represented by a box [] and possibly by a diamond $\langle\rangle$. The modality symbols can be empty or non-empty. The empty box [](necessarily or obligation) means the evaluation statement is true in every one-step successor of the current world of the model. Similarly, an empty diamond $\langle\rangle$ symbol modality (possibly modality or permission) means the evaluation of the modal formula is possible in some one-step successor of the current world of the model (see [BCT04], [AtC06], [BTC06]).

However, non-empty necessarily box $[\pi]\beta$ is used in propositional dynamic logic to mean every execution of π from the current state leads to the states bearing the information β. Similarly, the non-empty possibly modality $\langle\pi\rangle\,\beta$ means some terminating execution of π from the current state leads to the states bearing the information β [PBV10, p. 13].

The following complex relations also hold:

- If π_1 and π_2 are programs, then so is $\pi_1 \cup \pi_2$ – executes π_1 or π_2
- If π_1 and π_2 are programs, then so is $\pi_1; \pi_2$ – executes π_1 and then π_2
- If π is a program then so is π^* – executes π zero or finite number of times
- If π_1 and π_2 are programs, then so is $\pi_1 \cap \pi_2$ – executes π_1 and π_2 in parallel
- If β is a formula, then $\beta?$ is a program that test whether β holds, and if so continues; else stop

In order to model legal privacy risk, we group the normative values into three (legal competence, conduct and legal right) and introduce additional notation for them. We will use the following notations to represent the three normative groups. We represent the competence norm by ${}^{P}\langle\pi\rangle^{A}_{C}$, meaning the stakeholder P may perform the action π in order to achieve A. The notation ${}^{P}\langle\pi\rangle^{A}_{\Uparrow}$ represents legal right, meaning the stakeholder P may perform the action π in order to advance the interest of A. P is the same as A when one performs an action to advance his/her own interest. For norm of conduct ${}^{P}[\pi]^{A}$ will mean

ISBN 978-3-88579-286-4

the stakeholder P is obliged to perform the action π for A. P and A can be the same person, a role or an entity. In the case of program execution P is the name of the responsible stakeholders. A may represent a stakeholder and π is the program.

The following is the syntax and semantic of the hybrid logics language.

- Let the basic unanalyzed proposition or atomic formula $prop := p, q, r...and \top$ "$always\ true$", $\bot$ "$always\ false$".
- Let the set of nominal $NOM = \{n1, n2, n3...\}$.
- Let the set of state variables $SV = \{s1, s2, s3...\}$.
- The binary connective $\wedge$.
- The unary connective $\neg$.
- Let the finite set of programs $PI = \{\pi_1, \pi_2, \pi_3...\pi_n\}$.
- The unary operator $[\pi]$ where $\pi \in PI$.
- The unary operator $\langle\pi\rangle$ where $\pi \in PI$.
- The binder operator $\downarrow$
- The $@_x$ where x is a state variable or nominal.

$\theta := prop|\neg\varphi|(\varphi \wedge \phi)|(\varphi \vee \phi)|(\varphi \rightarrow \phi)|[\pi]\varphi|\langle\pi\rangle\varphi|[]\varphi|^P[\pi]^A$ where $\pi \in PI$
We write a hybrid modal logics formula that is true at a world w of a model $M = (W, R, V)$ as $M, w \models \varphi$. It follows that

- $M, w \models p$ iff $w \in V(p)$ where $p \in prop$
- $M, w \models \neg\varphi$ iff not $M, w \models \varphi$
- $M, w \models \varphi \wedge \phi$ iff $M, w \models \varphi$ and $M, w \models \phi$
- $M, w \models @_x\varphi$ iff $M, x \models \varphi$ where $x \in SV$
- $M, w \models \varphi \rightarrow \phi$ iff not $M, w \models \varphi$ or $M, w \models \phi$

We refer to this as Kripke semantics, named after Saul Kripke [BvB88].

5.1 A Case Example of Privacy Legal Risk Assessment

We consider an example of the application of the hybrid language for legal privacy risk assessment. We consider the DPD article 3(2) and article 23(1) for the legal privacy risk assessment. We manually extract normative values by following the steps in [KZB+07]. The result is shown in Table 1.

Rule No.	Norm Proposition (Rule)	Normative Phrase	Normative Value
R1	DPD article 3(2): This Directive shall not apply to the processing of personal data: in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing State in areas of criminal law, by a natural person in the course of a operation relates to State security matters) and the activities of the purely personal or household activity.	shall not	Not Obligation
R2	DPD aricle 23(1): Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act to this Directive incompatible with the national provisions adopted pursuant is entitled to receive compensation from the controller for the damage suffered	shall	obligation

Table 1: Legal Privacy Risk

We specify the legal privacy risk with the hybrid modal language described in the first part of this section using the model in Figure 2b. We assume that the transitions can occur in both directions of a world. A world has a set of propositions and is accessible from another world. We assume that each of the entities Legal Antecedent, Factual Consequent, Legal Consequent and Loss is accessible form other entities. Therefore, the entities Legal Antecedent, Factual Consequent, Legal Consequent and Loss are the possible worlds. We represent them by w_{la}, w_{fc}, w_{lc} and w_l respectively. The set of the possible worlds or the universe $W = \{w_{la}, w_{fc}, w_{lc}, w_l\}$. The analysis of a scenario or a legal proposition may lead to a program execution that may lead to a new state or world. Hence, it is possible to access a world from another world. We represent each state with a set of nominal. $Nominal = \{la, fc, lc, l\}$ represents the nominal for the worlds or states w_{la}, w_{fc}, w_{lc} and w_l respectively. The Table 2 and Table 3 exemplify the legal privacy specification and automation.

ID	Factual Proposition	Formula
F1	Distribution of someone's social website conversation may lead to non personal use	$@_l \langle \pi^* ? \rangle$

Table 2: Factual Specification

π^* represents a program that iterate through a series of factual propositions in order to make a transition decision.

ID	Legal Assessment	Normative Value	Formula
L1	Is distribution of someone's social website conversation illegal? (According to DPD article 3(2) (R1 in Table 1) the directive shall not apply to data processed for purely personal or household activity) (But the available fact contradicts R1)	Obligation (Contrary to the Rule R1)	$@_l^P [\pi_1^*; \pi_2^*]^A$
L2	Is non personal use of someone's social website data attract damages? (According to DPD article 23(1) (R2 in Table 1) violation of a privacy rule (R1) shall attract damages)	Obligation	$^P [\pi_5^*; \pi_6^*]^A \beta$ $\beta \in w_{fc}$

Table 3: Risk Tolerance

The iterations in the formulas in the Table 3 refer a scan through multiple legal sources and propositions. Thus, the expression $\pi_n^*; \pi_m^*$ means π_n^* is the iteration over legal sources and then iteration over legal propositions. The formula for possible legal privacy risk is as follows:

$Loss := @_l \langle \pi^*? \rangle \wedge @_l^P [\pi_1^*; \pi_2^*]^A \wedge^P [\pi_5^*; \pi_6^*]^A \beta \wedge \downarrow_x ([impact]\alpha \wedge {}^P \langle (\pi_7^* : \alpha)? \rangle_x^A)$
where $\alpha \in w_l c$

The formula, $Loss$ satisfied means the stakeholder can tolerate the legal privacy risk, otherwise the estimated loss is inconsistent with the objectives of the stakeholder and therefore we may transfer, avoid, mitigate or share the risk. The transition ${}^P [\pi_5^*; \pi_6^*]^A \beta$ leads to a state state satisfying β (the legal consequent state w_{lc} in this case). The state w_{lc} determines the risk impact α and makes a transition to the state that must satisfy α (the Loss state in this case). The expression $(\pi_7^* : \alpha)?$ compares the risk tolerance propositions π_7^* at the Loss state to the estimated damage α and makes a transition accordingly. The formula $Loss$ is a simple logical formalization of legal privacy risk. It highlights one of the possible ways of specifying legal privacy risk from technical viewpoint.

We may build on the technique in this article to automate the privacy risk of a SP. However, it is not clear if the current privacy legal regulations support the application of our technique for privacy risk in social media. The DPD was originally intended to regulate the activities of organizations or data controllers but people mainly use social media in their private capacity. Moreover, the DPD article (2b) [Com95] definition of data controller may not directly apply to the manner in which end users collect or process personal information in social media because the purpose for data processing and consent is not explicitly in social media. In addition, the DPD article 3(2) provides exception for personal data processing for personal or household activity. The opinion of the Article 29 Data Protection Working Party [Par09] is that end users would generally be protected under DPD article 3(2) (see also [Won09]) but may not be covered if their activity full outside the provision. This means our technique may apply if an end user uses social media data for non-private activity.

6 Conclusion

In this article, we propose an approach towards legal privacy risk assessments based on the CORAS risk assessment method. We consider the increased complexity of social media due to its nature of interdependant, meshed data controllers. We explain how legal privacy risk assessment differs from security risk assessment and demonstrate the possible technique for legal privacy risk automation. We proposed that legal privacy risk assessment automation involves extraction of normative values from legal text, analysis of facts and factual consequences, and the effects of legal norms on the analysis. We made an attempt towards a risk assessment automation based on the legal privacy principles that could reduce uncertainty in the legal privacy risk estimation and communication in social media. The possible risk assessment automation can enable end users of social media understand and assess their legal privacy risk with ease. Our future work will examine complex scenarios in the legal privacy risk assessment automation and how legal uncertainty may contribute to legal privacy risk assessment automation.

ISBN 978-3-88579-286-4

Acknowledgment: The work reported in this paper is part of the PETweb II project sponsored by the Research Council of Norway under grant 193030/S10.

References

[ANM09] Saeed Abu-Nimeh and Nancy R. Mead. Privacy Risk Assessment in Privacy Requirements Engineering. *Requirements Engineering and Law*, pages 17–18, 2009.

[AtC06] C. Areces and B. ten Cate. Hybrid Logics. In P. Blackburn, F. Wolter, and J. van Benthem, editors, *Handbook of Modal Logics*. Elsevier, 2006.

[Ave08] Terje Aven. A semi-quantitative approach to risk analysis, as an alternative to QRAs. *Reliability Engineering & System Safety*, 93(6):790 – 797, 2008.

[BCT04] Nicole Bidoit, Serenella Cerrito, and Virginie Thion. A First Step towards Modeling Semistructured Data in Hybrid Multimodal Logic. *Journal of Applied Non-Classical Logics*, 14(4):447–475, 2004.

[Ber03] Lucas Bergkamp. *uropean Community Law for the New Economy*. Intersentia Publishers, Antwerp Oxford New York, 2003. isbn:90-5095-229-1.

[BMAM08] Travis D. Breaux, Student Member, Annie I. Antón, and Senior Member. Analyzing regulatory rules for privacy and security requirements. *IEEE Transactions on Software Engineering*, 34:5–20, 2008.

[BTC06] Patrick Blackburn and Balder Ten Cate. Pure Extensions, Proof Rules, and Hybrid Axiomatics. *Studia Logica*, 84:277–322, 2006. A.: General Literature.

[Bul92] Eugenio Bulygin. On norms of competence. *Law and Philosophy*, 11(3), 1992.

[BvB88] Patrick Blackburn and Johan van Benthem. Modal Logic: A Semantic Perspective. *ETHICS*, 98:501–517, 1988.

[Com95] European Commission. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Technical report, 24-Oct-1995 1995.

[Cui07] Collete Cuijpers. "A Private Law Approach to Privacy; Mandatory Law". *SCRIPTed*, 4:4(318), 2007.

[Edw05] Lilian Edwards. *The New Legal Framework for E-Commerce in Europe*. Oxford and Portland, Hart Publishing, c/o International Specialized Book Services, 5804 NE Hassalo Street, Portland, Oregon, 97213-3644, USA, 2005. isbn 13:978-1-84113-451-2.

[Enc10] Deontic Logic IVR Encyclopedie. Deontic Logic. *IVR Encyclopedie*, 2010.

[Gar09] James Garson. Modal Logic. In Edward N. Zalta, editor, *The Stanford Encyclopedia of Philosophy*. Winter 2009 edition, 2009.

[Har94] H.L.A. Hart. *The Concept of Law*. Clarendon Press, Oxford, 2 edition, 1994. isbn:0-19-876123-6.

[ISA09] ISACA. *The Risk IT Practitioner Guide*. ISACA, 3701 Algonquin Road, Suite 1010 Rolling Meadows, IL 60008 USA, 2009. isbn: 978-1-60420-116-1.

[JS96] Andrew J. I. Jones and Marek J. Sergot. A Formal Characterisation of Institutionalised Power. *Logic Journal of the IGPL*, 4(3):427–443, 1996.

[KZB+07] Nadzeya Kiyavitskaya, Nicola Zeni, Travis D. Breaux, Annie I. Antón, James R. Cordy, Luisa Mich, and John Mylopoulos. Extracting rights and obligations from regulations: toward a tool-supported process. In *Proceedings of the twenty-second IEEE/ACM international conference on Automated software engineering*, ASE '07, pages 429–432, New York, NY, USA, 2007. ACM.

[Mah10] Tobias Mahler. *Legal Risk Management Developing and Evaluating Elements of a Method for Proactive Legal Analyses, With a Particular Focus on Contracts*. Monograph, The Faculty of Law, University of Oslo, Postboks 6706 St Olavs Plass, 0130 Oslo Norway, February 2010.

[MMM+08] Raimundas Matulevičius, Nicolas Mayer, Haralambos Mouratidis, Eric Dubois, Patrick Heymans, and Nicolas Genon. Adapting Secure Tropos for Security Risk Management in the Early Phases of Information Systems Development. In *Proceedings of the 20th international conference on Advanced Information Systems Engineering*, CAiSE '08, pages 541–555, Berlin, Heidelberg, 2008. Springer-Verlag.

[MSL11] Ketil Stølen Mass Soldal Lund, Bjørnar Solhaug. *Model-Driven Risk Analysis, The CORAS Approach*. Springer, 1 edition, 2011. 978-3-642-12322-1.

[Off09] Information Commissioner Office. Privacy Impact Assessment Handbook - Version 2. Technical report, ICO, London, UK, June 2009.

[OM07] Thomas Olsen and Tobias Mahler. Identity Management and Data Protection Law: Risk, Responsibility and Compliance in 'Circles of Trust'. *Computer Law & Security Report*, 23(4):342–351, 2007.

[Par09] Art.29 Data Protection Working Party. Opinion 5/2009 on online social networking, 2009. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf.

[PBV10] Maarten de Rijke Patrick Blackburn and Yde Venema. *Modal Logic*. Cambridge University Press, 2010. isbn:978-0-521-80200-0.

[Sar06] GIOVANNI Sartor. Fundamental legal concepts: A formal and teleological characterisation. *Artificial Intelligence and Law*, 14:101–142, 2006.

[TMM05] Doris R. Kirby Tracy Mitrano and Leslie Maltz. "What does privacy have to do with it?: privacy risk assessment". 2005.

[VLM+05] Fredrik Vraalsen, Mass Soldal Lund, Tobias Mahler, Xavier Parent, and Ketil Stølen. Specifying Legal Risk Scenarios Using the CORAS Threat Modelling Language. In Peter Herrmann, Issarny, and Simon Shiu, editors, *Trust Management*, volume 3477 of *Lecture Notes in Computer Science*, pages 45–60. Springer Berlin / Heidelberg, 2005. 10.1007/11429760_4.

[Wan05] Andy Ju An Wang. Information security models and metrics. In *ACM-SE 43: Proceedings of the 43rd annual Southeast regional conference*, pages 178–184, New York, NY, USA, 2005. ACM.

[Won09] Rebecca Wong. Social networking: a conceptual analysis of a data controller. *Communications Law, Vol. 14, No. 5*, pages 142–149, 2009.