Noname manuscript No.
(will be inserted by the editor)

Privacy requirements elicitation: A systematic literature review and perception analysis of IT practitioners

Received: date / Accepted: date

Abstract Context: During the software development process and throughout the software lifecycle, organizations must guarantee users' privacy by protecting personal data. There are several studies in the literature proposing methodologies, techniques, and tools for privacy requirements elicitation. These studies report that practitioners must use systematic approaches to specify these requirements during initial software development activities to avoid users' data privacy breaches. **Objective**: The main goal of this study is to identify which methodologies, techniques, and tools are used in privacy requirements elicitation in the literature. We have also investigated Information Technology (IT) practitioners' perceptions regarding the methodologies, techniques, and tools identified in the literature. **Method**: We have carried out a systematic literature review (SLR) to identify the methodologies, techniques, and tools used for privacy requirements elicitation. Besides, we have surveyed IT practitioners to understand their perception of using these techniques and tools in the software development process. **Results**: We have found several methodologies, techniques, and tools proposed in the literature to carry out privacy requirements elicitation. Out of 78 studies cataloged within the SLR, most of them did not verify their methodologies and techniques in a practical case study or illustrative contexts (38 studies), and less than 35% of them (26 studies) experimented with their propositions within an industry context. The Privacy Safeguard method (PriS) is the best known among the 198 practitioners in the industry who participated in the survey. Moreover, use cases and user story are their most-used techniques. **Conclusion**: This qualitative study shows a perception of IT practitioners different from that presented in other research papers, and suggests that methodologies, techniques, and tools play an important role in IT practitioners' perceptions about privacy requirements elicitation.

Address(es) of author(s) should be given

Keywords Privacy Requirements Elicitation · Systematic Literature Review · Methodologies · Techniques · Tools

1 Supplementary Material

ID	Reference	Methodologies	Techniques	Tools
S1	Yu and Cysneiros [77]	i* Model; Non-Functional Requirements (NFR) Framework.		
S2	He et al. [27]	Discretionary and Mandatory Access Controls (DAC and MAC); Privacy-Aware Role-Based Access Control (PARBAC).		Specific, Measurable, Attainable, Realizable, and Traceable (SMaRT).
S3	Liu et al. [41]	i* Model; Agent-Based Model; Alloy Language; Agent-Oriented Modeling Framework.		
S4	Jensen et al. [31]	Goal-Oriented Approach.		STRuctured Analysis for Privacy (STRAP) Tool.
S5	Sindre and Opdahl [69]		Misuse Case.	
S6	Mouratidis and Giorgini [48]	i* Model; Secure Tropos.		T-Tool.
S7	Kalloniatis et al. [33]	Privacy Safeguard Method (PriS).		
S8	Tøndel et al. [72]	NFR Framework.	Misuse Case; Use case.	
S9	Miyazaki et al. [46]	Development Life Cycle Models and Cost.	Questionnaire; Use Case; Flow Charts.	Privacy Requirements Elicitation Technique (PRET) Tool.

S10	Kalloniatis et al. [34]	PriS Conceptual Framework.		
S11	Kalloniatis et al. [35]	Goal Model; Directed Acyclic Graph.		PriS Tool.
S12	Bijwe and Mead [11]	Goal-Based Requirements Analysis Method (GBRAM); Pattern-Based Approach (PBA); E-Commerce Personalization Approach (ECPA); Soft Systems Methodology (SSM); Feature-Oriented Domain Analysis (FODA).	Use Case; Misuse Case; Attack Trees; User-Role Hierarchies (URH); System Architecture Diagrams (SAD); Interviews.	PRET Tool.
S13	Islam et al. [29]	Secure Tropos; Goal Driven Security Risk Management (GSRM).		
S14	Deng et al. [16]	Linkability, Identifiability, Non-repudiation, Detectability, Information Disclosure, Content Unawareness and Policy/Consent Non-compliance (LINDDUN).	Data Flow Diagrams (DFD); Use Case.	
S15	Kalloniatis et al. [36]	Pris Extension.		Pris Tool.

S16	Mead et al. [45]	PRET; Security Quality Requirements Engineering (SQUARE); Soft Systems Methodology (SSM); Quality Function Deployment (QFD); Controlled Requirements Expression (CORE); Issue-Based Information Systems (IBIS); FODA; Critical Discourse Analysis (CDA); Accelerated Requirements Method (ARM); Reusable Legal Requirements; GBRAM; PBA; ECPA.	Misuse Case; Joint Application Development (JAD); Questionnaire.	
S17	Mouratidis et al. [49]	NFR Framework; i* Model; Secure Tropos; Keep All Objectives Satisfied (KAOS); Goal-Based Requirements Analysis Method (GBRAM); Role Based Access Control (RBAC); Moffett-Nuseibeh (M-N) Framework; STRuctured Analysis for Privacy (STRAP); Privacy Safeguard (PriS).		
S18	Beckers [10]	Conceptual Framework for Security Requirements Engineering (CF); PriS; LINDDUN; Privacy-Friendly System Design from Spiekermann (FPRSD).		

S19	Neureiter et al. [53]	Reliability, Availability, Maintainability and Safety (RAMS); Privacy-RAMS; LINDDUN.		
S20	Kalloniatis et al. [37]	Secure Tropos; Pris.		
S21	Amorim et al. [5]	Privacy by Design; Digital Image Analysis (DIA).		
S22	Radics et al. [64]	Poolsappasit and Ray's Framework; Sensor-Safe and MAPaS framework; Beckers' Method; LINDDUN; PriS; Model by Hong; Privacy Requirements Engineering Process (PREPProcess).		
S23	Martín et al. [43]	Privacy by Design; Privacy Enhancing Technology (PET), Pris; i* Model.		OASIS-Privacy Management Reference Model Methodology (PMRM) Tools.
S24	Breaux et al. [12]		Survey; Interview; DFD.	
S25	Ganji et al. [21]	NFR Framework; i* Model; Secure Tropos; KAOS; GBRAM; RBAC; M-N Framework, Bellotti-Sellen Framework, STRAP; PriS, Caprice, SecuriTas, Easy Win-Win.		
S26	Notario et al. [54]	Goal-Oriented; System Analysis Approach; Privacy by Design.		

S27	Gharib et al. [24]	Questionnaire-Based Requirements Elicitation; Scenario Based Requirements Elicitation.		
S28	Argyropoulos et al. [7]	Secure Tropos Approach; Secure Tropos.	Business Process Model and Notation (BPMN).	
S29	Mukisa and Rashid [51]	LINDDUN.		
S30	Pattakou et al. [55]	SQUARE; Model Oriented Security Requirements Engineering (MOSRE); Security Requirements Engineering Framework (SREF); Security Requirements Engineering Process (SREP); Secure Tropos; KAOS; Problem-based Security Requirements Elicitation (PreSure); LINDDUN; SQUARE; PriS.	BPMN.	
S31	Diamantopoulou et al. [17]	Secure Tropos Graphical Notation.		
S32	Gharib et al. [25]	Privacy by Design.	Unified Modeling Language (UML) Diagram.	
S33	Gharib and Mylopoulos [23]	COPri - a Core Ontology for Privacy Requirements Engineering.	BPMN.	
S34	Islam et al. [30]		UML Diagram; Use Case.	
S35	Junior et al. [32]		Questionnaire; Personas; User Story.	

S36	Pattakou et al. [56]	LINDDUN; SQUARE; PriS; RBAC; STRAP; Secure Tropos; PriS; i* Model; PRET.		PriS Tool.
S37	da Silva et al. [68]	Design of Crowdsourcing.		
S38	Mai et al. [42]	Natural Language Processing; Gamification.	Use Case; UML Diagram.	Restricted Misuse Case Modeling - Verifier (RMCM-V) Tool.
S39	Ayala-Rivera and Pasquale [8]	Business Analysis Body of Knowledge (BABOK).	Use Case; Questionnaire.	SMART Tool.
S40	Levy and Hadar [39]	Design Thinking.	Empathy Map.	
S41	Coles et al. [15]	Process Based on Computer Aided Integration of Requirements and Information Security (CAIRIS).	Use case; Personas; UML Diagrams; DFD; Semi-Structured Interview.	Tool Supported Data Protection Impact Assessment (DPIA).
S42	Peixoto and Silva [59]	Goal-Oriented Modeling Language.	UML Diagram; Survey.	

S43	Lim et al. [40]		Interview; Questionnaire; Brainstorming; Prototype; Use Case; Workshop; Affinity Mapping; Crowdsourcing Survey; Data Mining; Content Analysis; Cultural Probe; Ethnographic Data; Focal Group; Scenario; Roles; Service Blueprint.	
S44	Peixoto et al. [57]	Privacy Criteria Method (PCM).	User Story.	
S45	Netto et al. [52]		Interview; Case Study; Focus Group.	
S46	García-Mireles et al. [22]	PriS Method; Privacy by Design; LINDDUN; General Data Protection Regulation (GDPR).		
S47	Mohammadi et al. [47]	ISO/IEC 29100; GDPR; SPARQL, a query language for triple stores.		
S48	Veseli et al. [75]	Framework LINDDUN.	DFD.	
S49	Rösch et al. [65]	GDPR.		
S50	Bartolini et al. [9]	Conceptual Model of GDPR-Focused User Stories.	User Story.	

S51	Pullonen et al. [63]	Privacy-Oriented Goals; Privacy-Enhanced BPMN (PE-BPMN).	BPMN.	
S52	Stach and Steimle [70]	Recommender-Based Privacy Requirements Elicitation (EPICUREAN) and Privacy System for Internet of Things Applications (PATRON); Privacy by Design.	Interviews; Modeling and Data Mining Techniques.	
S53	Tsohou et al. [73]		Questionnaire; Interview.	
S54	Pullonen et al. [63]		BPMN.	
S55	Ahmadian et al. [2]		UML Diagram.	
S56	Vilela et al. [76]	System Theoretic Process Analysis (STPA); i* Model.		
S57	Mavroeidi et al. [44]	GDPR.	UML Diagram.	
S58	Peixoto et al. [57]	Privacy criteria Method.	User Story.	PCM Tool.
S59	Ehécatl Morales-Trujillo et al. [18]	Privacy by Design; GDPR.		
S60	Ferraris and Gago [19]	JSON-Based Requirement Elicitation; Security, Availability, Privacy, Identity and Safety (TrUStAPIS); K-Model proposed in previous work Ferraris et al. [20].		
S61	Mouratidis et al. [50]	Cloud Security Analysis; Security Mitigation Analysis and Transparency Analysis; SectroCloud Module.		

S62	Perera et al. [61]	Set of Guidelines Generated by the Adequacy of Privacy by Design for the Context of Internet Of Things.		
S63	Peixoto [58]	PCM.	User Story.	PCM Tool.
S64	Salnitri et al. [66]	Security, Privacy and Trust Approach (SePTA); Goal-Based Modelling Languages; Socio-Technical Security Modelling Language (STS-ml) Diagram; Secure Tropos; i* Model.	BPMN.	STS-Tool and SecTro Tool.
S65	Carvalho et al. [14]	i* Model.	Survey; Questionnaire.	
S66	Peixoto et al. [60]	iStar; Secure Tropos; Problem Frames; NFR Framework; SI* Modelling; GRL; Threat Model; KAOS; SecBPMN-ml; UML4PF.	Use Case; DFD.	
S67	Ahmadian [1]	Model-Based Privacy by Design; Model-Based Cost Estimation; PET; RAMS; CARiSMA.	UML Diagram.	
S68	Canedo et al. [13]		User Story; Use Case; Interview; BPMN.	
S69	He et al. [28]		Questionnaire.	Amazon Mechanical Turk.
S70	Tsohou et al. [74]	Privacy by Design; Secure Tropos.	Questionnaire; Interview; User Story.	SecTro Tool.
S71	Tomashchuk et al. [71]	GDPR; Chinese Cybersecurity Act.	Case Study; DFD.	
S72	Piras et al. [62]	Secure Tropos.	Questionnaire.	STS-Tool.
S73	Akil et al. [3]	GDPR.	Use Case.	

S74	Gharib et al. [26]	GDPR.	UML Diagram.	SPARQL Tool.
S75	Sangaroonsilp et al. [67]	GDPR; ISO/IEC 29100.		
S76	Ansari et al. [6]	Security Threat Oriented Requirements Engineering (STORE); LINDDUN.	Interview; Brainstorming; Questionnaire.	
S77	Alkubaisy et al. [4]	Secure Tropos Methodology; DEFeND Platform; ConfIS Framework.	Survey.	IDEMIX Tool; SecTro Tool.
S78	Kitsiou et al. [38]	Privacy by Design.	Questionnaire.	

Table 1: Primary studies selected from 2002 to 2021

References

1. Ahmadian A (2020) Model-based privacy by design. PhD thesis, University of Koblenz and Landau, Germany
2. Ahmadian AS, Strüber D, Jürjens J (2019) Privacy-enhanced system design modeling based on privacy features. In: Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing, SAC 2019, Limassol, Cyprus, April 8-12, 2019, https://doi.org/10.1145/3297280.3297431, https://dblp.org/rec/conf/sac/Ahmadian0J19.bib, pp 1492–1499, DOI 10.1145/3297280.3297431
3. Akil M, Islami L, Fischer-Hübner S, Martucci LA, Zuccato A (2020) Privacy-preserving identifiers for iot: A systematic literature review. IEEE Access 8:168470–168485
4. Alkubaisy D, Piras L, Al-Obeidallah MG, Cox K, Mouratidis H (2021) Confis: A tool for privacy and security analysis and conflict resolution for supporting GDPR compliance through privacy-by-design. In: Ali R, Kaindl H, Maciaszek LA (eds) Proceedings of the 16th International Conference on Evaluation of Novel Approaches to Software Engineering, ENASE 2021, Online Streaming, April 26-27, 2021, SCITEPRESS, pp 80–91, DOI 10.5220/0010406100800091, URL `https://doi.org/10.5220/0010406100800091`
5. Amorim JA, Åhlfeldt R, Gustavsson PM, Andler SF (2013) Privacy and security in cyberspace: Training perspectives on the personal data ecosystem. In: 2013 European Intelligence and Security Informatics Conference, Uppsala, Sweden, August 12-14, 2013, https://doi.org/10.1109/EISIC.2013.30, https://dblp.org/rec/conf/eisic/AmorimAGA13.bib, pp 139–142, DOI 10.1109/EISIC.2013.30
6. Ansari MTJ, Baz A, Alhakami H, Alhakami W, Kumar R, Khan RA (2021) P-store: Extension of store methodology to elicit privacy requirements. Arabian Journal for Science and Engineering pp 1–24
7. Argyropoulos N, Shei S, Kalloniatis C, Mouratidis H, Delaney AJ, Fish A, Gritzalis S (2017) A semi-automatic approach for eliciting cloud security and privacy requirements. In: HICSS, ScholarSpace / AIS Electronic Library (AISeL), http://hdl.handle.net/10125/41749, pp 1–10
8. Ayala-Rivera V, Pasquale L (2018) The grace period has ended: An approach to operationalize GDPR requirements. In: RE, IEEE Computer Society, 10.1109/RE.2018.00023, pp 136–146

9. Bartolini C, Daoudagh S, Lenzini G, Marchetti E (2019) Gdpr-based user stories in the access control perspective. In: QUATIC, Springer, https://doi.org/10.1007/978-3-030-29238-6_1, Communications in Computer and Information Science, vol 1010, pp 3–17
10. Beckers K (2012) Comparing privacy requirements engineering approaches. In: Seventh International Conference on Availability, Reliability and Security, Prague, ARES 2012, Czech Republic, August 20-24, 2012, IEEE, https://dblp.org/rec/conf/IEEEares/Beckers12.bib, pp 574–581, DOI 10.1109/ARES.2012.29, URL https://doi.org/10.1109/ARES.2012.29
11. Bijwe A, Mead N (2010) Adapting the square process for privacy requirements engineering (cmu/sei-2010-tn-022)
12. Breaux TD, Hibshi H, Rao A (2014) Eddy, a formal language for specifying and analyzing data flow specifications for conflicting privacy requirements. Requir Eng 19(3):281–307
13. Canedo ED, Calazans ATS, Masson ETS, Costa PHT, Lima F (2020) Perceptions of ICT practitioners regarding software privacy. Entropy 22(4):429
14. Carvalho RM, Andrade RMC, Lelli V, Silva EG, de Oliveira KM (2020) What about catalogs of non-functional requirements? In: REFSQ Workshops, CEUR Workshop Proceedings, CEUR-WS.org, vol 2584, pp 1–6
15. Coles J, Faily S, Ki-Aries D (2018) Tool-supporting data protection impact assessments with CAIRIS. In: ESPRE@RE, IEEE, 10.1109/ESPRE.2018.00010, pp 21–27
16. Deng M, Wuyts K, Scandariato R, Preneel B, Joosen W (2011) A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. Requir Eng 16(1):3–32
17. Diamantopoulou V, Pavlidis M, Mouratidis H (2017) Evaluation of a security and privacy requirements methodology using the physics of notation. In: CyberICPS/SECPRE@ESORICS, Springer, https://doi.org/10.1007/978-3-319-72817-9_14, Lecture Notes in Computer Science, vol 10683, pp 210–225
18. Ehécatl Morales-Trujillo M, García-Mireles GA, Matla-Cruz EO, Piattini M (2019) A systematic mapping study on privacy by design in software engineering. Clei Electronic Journal
19. Ferraris D, Gago MCF (2020) Trustapis: a trust requirements elicitation method for iot. Int J Inf Sec 19(1):111–127, DOI 10.1007/s10207-019-00438-x, URL https://doi.org/10.1007/s10207-019-00438-x
20. Ferraris D, Gago MCF, López J (2018) A trust-by-design framework for the internet of things. In: 9th IFIP International Conference on New Technologies, Mobility and Security, NTMS 2018, Paris, France, February 26-28, 2018, IEEE, https://dblp.org/rec/conf/ntms/FerrarisGL18.bib, pp 1–4, DOI 10.1109/NTMS.2018.8328674, URL https://doi.org/10.1109/NTMS.2018.8328674
21. Ganji D, Mouratidis H, Gheytassi SM, Petridis M (2015) Conflicts between security and privacy measures in software requirements engineering. In: Global Security, Safety and Sustainability: Tomorrow's Challenges of Cyber Security - 10th International Conference, ICGS3 2015, London, UK, September 15-17, 2015. Proceedings, Springer, https://dblp.org/rec/conf/icgs3/GanjiMGP15.bib, pp 323–334, DOI 10.1007/978-3-319-23276-8_29, URL https://doi.org/10.1007/978-3-319-23276-8_29
22. García-Mireles GA, Ehécatl Morales-Trujillo M, Piattini M, Matla-Cruz EO (2019) A systematic mapping study on privacy by design in software engineering. Clei Electronic Journal 22(1):1–20
23. Gharib M, Mylopoulos J (2018) A core ontology for privacy requirements engineering. CoRR abs/1811.12621:1–44, URL http://arxiv.org/abs/1811.12621, 1811.12621
24. Gharib M, Salnitri M, Paja E, Giorgini P, Mouratidis H, Pavlidis M, Ruiz JF, Fernandez S, Siria AD (2016) Privacy requirements: Findings and lessons learned in developing a privacy platform. In: RE, IEEE Computer Society, 10.1109/RE.2016.13, pp 256–265
25. Gharib M, Giorgini P, Mylopoulos J (2017) Towards an ontology for privacy requirements via a systematic literature review. In: Conceptual Modeling - 36th International Conference, ER 2017, Valencia, Spain, November 6-9, 2017, Proceedings, IEEE, https://dblp.org/rec/conf/er/GharibGM17.bib, pp 193–208, DOI 10.1007/978-3-319-69904-2_16, URL https://doi.org/10.1007/978-3-319-69904-2_16

26. Gharib M, Giorgini P, Mylopoulos J (2021) Copri v.2 - A core ontology for privacy requirements. Data Knowl Eng 133:101888
27. He Q, Antón AI, et al. (2003) A framework for modeling privacy requirements in role engineering. In: Procedures of REFSQ, REFSQ, https://core.ac.uk/display/21027630, vol 3, pp 137–146
28. He Y, Bahirat P, Knijnenburg BP, Menon A (2020) A data-driven approach to designing for privacy in household iot. ACM Trans Interact Intell Syst 10(1):10:1–10:47, DOI 10.1145/3241378, URL https://doi.org/10.1145/3241378
29. Islam S, Mouratidis H, Wagner S (2010) Towards a framework to elicit and manage security and privacy requirements from laws and regulations. In: Requirements Engineering: Foundation for Software Quality, 16th International Working Conference, REFSQ 2010, Essen, Germany, June 30 - July 2, 2010. Proceedings, IEEE, https://dblp.org/rec/conf/refsq/IslamMW10.bib, pp 255–261, DOI 10.1007/978-3-642-14192-8_23, URL https://doi.org/10.1007/978-3-642-14192-8_23
30. Islam S, Ouedraogo M, Kalloniatis C, Mouratidis H, Gritzalis S (2018) Assurance of security and privacy requirements for cloud deployment models. IEEE Trans Cloud Computing 6(2):387–400, DOI 10.1109/TCC.2015.2511719, URL https://doi.org/10.1109/TCC.2015.2511719
31. Jensen C, Tullio J, Potts C, Mynatt ED (2005) Strap: a structured analysis framework for privacy. Tech. rep., Georgia Institute of Technology
32. Junior DPS, de Souza PC, de Jesus Gonçalves TA (2018) Early privacy: Approximating mental models in the definition of privacy requirements in systems design. In: Proceedings of the 17th Brazilian Symposium on Human Factors in Computing Systems, IHC 2018, Belém, Brazil, October 22-26, 2018, ACM, https://dblp.org/rec/conf/ihc/JuniorSG18.bib, pp 19:1–19:10, DOI 10.1145/3274192.3274211, URL https://doi.org/10.1145/3274192.3274211
33. Kalloniatis C, Kavakli E, Gritzalis S (2007) Using privacy process patterns for incorporating privacy requirements into the system design process. In: Proceedings of the The Second International Conference on Availability, Reliability and Security, ARES 2007, The International Dependability Conference - Bridging Theory and Practice, April 10-13 2007, Vienna, Austria, IEEE, https://dblp.org/rec/conf/IEEEares/KalloniatisKG07.bib, pp 1009–1017, DOI 10.1109/ARES.2007.156, URL https://doi.org/10.1109/ARES.2007.156
34. Kalloniatis C, Kavakli E, Gritzalis S (2008) Addressing privacy requirements in system design: the pris method. Requir Eng 13(3):241–255, DOI 10.1007/s00766-008-0067-3, URL https://doi.org/10.1007/s00766-008-0067-3
35. Kalloniatis C, Kavakli E, Kontellis E (2009) Pris tool: A case tool for privacy-oriented requirements engineering. In: MCIS, Athens University of Economics and Business / AISeL, https://aisel.aisnet.org/mcis2009/71/, p 71
36. Kalloniatis C, Belsis P, Gritzalis S (2011) A soft computing approach for privacy requirements engineering: The pris framework. Appl Soft Comput 11(7):4341–4348, DOI 10.1016/j.asoc.2010.10.012, URL https://doi.org/10.1016/j.asoc.2010.10.012
37. Kalloniatis C, Mouratidis H, Islam S (2013) Evaluating cloud deployment scenarios based on security and privacy requirements. Requir Eng 18(4):299–319
38. Kitsiou A, Tzortzaki E, Kalloniatis C, Gritzalis S (2021) Identifying privacy related requirements for the design of self-adaptive privacy protections schemes in social networks. Future Internet 13(2):23, DOI 10.3390/fi13020023, URL https://doi.org/10.3390/fi13020023
39. Levy M, Hadar I (2018) The importance of empathy for analyzing privacy requirements. In: ESPRE@RE, IEEE, 10.1109/ESPRE.2018.00008, pp 9–13
40. Lim T, Chua F, Tajuddin BB (2018) Elicitation techniques for internet of things applications requirements: A systematic review. In: ICNCC, ACM, https://doi.org/10.1145/3301326.3301360, pp 182–188
41. Liu L, Yu ESK, Mylopoulos J (2003) Security and privacy requirements analysis within a social setting. In: RE, IEEE Computer Society, 10.1109/ICRE.2003.1232746, pp 151–161
42. Mai PX, Goknil A, Shar LK, Pastore F, Briand LC, Shaame S (2018) Modeling security and privacy requirements: a use case-driven approach. Inf Softw Technol 100:165–182

43. Martín YS, Del Alamo JM, Yelmo JC (2014) Engineering privacy requirements valuable lessons from another realm. In: 2014 IEEE 1st International Workshop on Evolving Security and Privacy Requirements Engineering (ESPRE), IEEE, 10.1109/ESPRE.2014.6890523, pp 19–24
44. Mavroeidi A, Kitsiou A, Kalloniatis C (2019) The interrelation of game elements and privacy requirements for the design of a system: A metamodel. In: TrustBus, Springer, https://doi.org/10.1007/978-3-030-27813-7_8, Lecture Notes in Computer Science, vol 11711, pp 110–125
45. Mead NR, Miyazaki S, Zhan J (2011) Integrating privacy requirements considerations into a security requirements engineering method and tool. IJIPSI 1(1):106–126, DOI 10.1504/IJIPSI.2011.043733, URL https://doi.org/10.1504/IJIPSI.2011.043733
46. Miyazaki S, Mead NR, Zhan J (2008) Computer-aided privacy requirements elicitation technique. In: APSCC, IEEE Computer Society, 10.1109/APSCC.2008.263, pp 367–372
47. Mohammadi NG, Leicht J, Ulfat-Bunyadi N, Heisel M (2019) Privacy policy specification framework for addressing end-users' privacy requirements. In: Trust, Privacy and Security in Digital Business - 16th International Conference, TrustBus 2019, Linz, Austria, August 26-29, 2019, Proceedings, Springer, https://dblp.org/rec/conf/trustbus/MohammadiLUH19.bib, pp 46–62, DOI 10.1007/978-3-030-27813-7_4, URL https://doi.org/10.1007/978-3-030-27813-7_4
48. Mouratidis H, Giorgini P (2007) Secure tropos: a security-oriented extension of the tropos methodology. International Journal of Software Engineering and Knowledge Engineering 17(2):285–309, DOI 10.1142/S0218194007003240, URL https://doi.org/10.1142/S0218194007003240
49. Mouratidis H, Kalloniatis C, Islam S, Huget M, Gritzalis S (2012) Aligning security and privacy to support the development of secure information systems. J UCS 18(12):1608–1627
50. Mouratidis H, Shei S, Delaney AJ (2020) A security requirements modelling language for cloud computing environments. Software and Systems Modeling 19(2):271–295, DOI 10.1007/s10270-019-00747-8, URL https://doi.org/10.1007/s10270-019-00747-8
51. Mukisa SS, Rashid A (2017) Challenges of privacy requirements modelling in V2X applications: A telematic insurance case study. In: IEEE 25th International Requirements Engineering Conference Workshops, RE 2017 Workshops, Lisbon, Portugal, September 4-8, 2017, IEEE, https://dblp.org/rec/conf/re/MukisaR17.bib, pp 97–103, DOI 10.1109/REW.2017.48, URL https://doi.org/10.1109/REW.2017.48
52. Netto D, Peixoto MM, Silva C (2019) Privacy and security in requirements engineering: Results from a systematic literature mapping. In: WER, Editora PUC-Rio, http://wer.inf.puc-rio.br/WERpapers/artigos/artigos_WER19/WER_2019_paper_14.pdf, pp 1–15
53. Neureiter C, Eibl G, Veichtlbauer A, Engel D (2013) Towards a framework for engineering smart-grid-specific privacy requirements. In: IECON 2013 - 39th Annual Conference of the IEEE Industrial Electronics Society, Vienna, Austria, November 10-13, 2013, IEEE, https://dblp.org/rec/conf/iecon/NeureiterEVE13.bib, pp 4803–4808, DOI 10.1109/IECON.2013.6699912, URL https://doi.org/10.1109/IECON.2013.6699912
54. Notario N, Crespo A, Martín YS, del Álamo JM, Métayer DL, Antignac T, Kung A, Kroener I, Wright D (2015) PRIPARE: integrating privacy best practices into a privacy engineering methodology. In: IEEE Symposium on Security and Privacy Workshops, IEEE Computer Society, 10.1109/SPW.2015.22, pp 151–158
55. Pattakou A, Kalloniatis C, Gritzalis S (2017) Security and privacy requirements engineering methods for traditional and cloud-based systems: a review. CLOUD COMPUTING 2017 155:1–7
56. Pattakou A, Mavroeidi AG, Diamantopoulou V, Kalloniatis C, Gritzalis S (2018) Towards the design of usable privacy by design methodologies. In: 2018 IEEE 5th International Workshop on Evolving Security & Privacy Requirements Engineering (ESPRE), IEEE, 10.1109/ESPRE.2018.00007, pp 1–8
57. Peixoto M, Silva C, Lima R, Araújo J, Gorschek T, Silva J (2019) Pcm tool: Privacy requirements specification in agile software development. In: Anais Estendidos da X Conferência Brasileira de Software: Teoria e Prática, SBC, 10.5753/cb-

soft_estendido.2019.7666, pp 108–113
58. Peixoto MM (2020) Privacy requirements engineering in agile software development: a specification method. In: Joint Proceedings of REFSQ-2020 Workshops, Doctoral Symposium, Live Studies Track, and Poster Track co-located with the 26th International Conference on Requirements Engineering: Foundation for Software Quality (REFSQ 2020), Pisa, Italy, March 24, 2020, IEEE, https://dblp.org/rec/conf/refsq/Peixoto20.bib, pp 1–7, URL http://ceur-ws.org/Vol-2584/DS-paper1.pdf
59. Peixoto MM, Silva C (2018) Specifying privacy requirements with goal-oriented modeling languages. In: Proceedings of the XXXII Brazilian Symposium on Software Engineering, SBES 2018, Sao Carlos, Brazil, September 17-21, 2018, ACM, https://dblp.org/rec/conf/sbes/PeixotoS18.bib, pp 112–121, DOI 10.1145/3266237.3266270, URL https://doi.org/10.1145/3266237.3266270
60. Peixoto MM, Silva C, Maia H, Araújo J (2020) Towards a catalog of privacy related concepts. In: REFSQ Workshops, CEUR-WS.org, http://ceur-ws.org/Vol-2584/PT-paper5.pdf, CEUR Workshop Proceedings, vol 2584, pp 1–6
61. Perera C, Barhamgi M, Bandara AK, Azad MA, Price BA, Nuseibeh B (2020) Designing privacy-aware internet of things applications. Inf Sci 512:238–257, DOI 10.1016/j.ins.2019.09.061, URL https://doi.org/10.1016/j.ins.2019.09.061
62. Piras L, Calabrese F, Giorgini P (2020) Applying acceptance requirements to requirements modeling tools via gamification: A case study on privacy and security. In: PoEM, Springer, Lecture Notes in Business Information Processing, vol 400, pp 366–376
63. Pullonen P, Tom J, Matulevicius R, Toots A (2019) Privacy-enhanced BPMN: enabling data privacy analysis in business processes models. Software and Systems Modeling 18(6):3235–3264, DOI 10.1007/s10270-019-00718-z, URL https://doi.org/10.1007/s10270-019-00718-z
64. Radics PJ, Gracanin D, Kafura DG (2013) Preprocess before you build: Introducing a framework for privacy requirements engineering. In: International Conference on Social Computing, SocialCom 2013, SocialCom/PASSAT/BigData/EconCom/BioMedCom 2013, Washington, DC, USA, 8-14 September, 2013, IEEE, https://dblp.org/rec/conf/socialcom/RadicsGK13.bib, pp 564–569, DOI 10.1109/SocialCom.2013.85, URL https://doi.org/10.1109/SocialCom.2013.85
65. Rösch D, Schuster T, Waidelich L, Alpers S (2019) Privacy control patterns for compliant application of GDPR. In: 25th Americas Conference on Information Systems, AMCIS 2019, Cancún, Mexico, August 15-17, 2019, AISEL, https://dblp.org/rec/conf/amcis/RoschSWA19.bib, pp 1–10, URL https://aisel.aisnet.org/amcis2019/info_security_privacy/info_security_privacy/27
66. Salnitri M, Angelopoulos K, Pavlidis M, Diamantopoulou V, Mouratidis H, Giorgini P (2020) Modelling the interplay of security, privacy and trust in sociotechnical systems: a computer-aided design approach. Software and Systems Modeling 19(2):467–491
67. Sangaroonsilp P, Dam HK, Choetkiertikul M, Ragkhitwetsagul C, Ghose A (2021) A taxonomy for mining and classifying privacy requirements in issue reports. CoRR abs/2101.01298
68. da Silva M, Viterbo J, Bernardini F, Maciel C (2018) Identifying privacy functional requirements for crowdsourcing applications in smart cities. In: ISI, IEEE, 10.1109/ISI.2018.8587316, pp 106–111
69. Sindre G, Opdahl AL (2005) Eliciting security requirements with misuse cases. Requir Eng 10(1):34–44, URL http://www.springerlink.com/index/10.1007/s00766-004-0194-4
70. Stach C, Steimle F (2019) Recommender-based privacy requirements elicitation - EPICUREAN: an approach to simplify privacy settings in iot applications with respect to the GDPR. In: SAC, ACM, https://doi.org/10.1145/3297280.3297432, pp 1500–1507
71. Tomashchuk O, Li Y, Van Landuyt D, Joosen W (2020) Operationalization of privacy and security requirements for ehealth iot applications in the context of gdpr and csl. In: Antunes L, Naldi M, Italiano GF, Rannenberg K, Drogkaris P (eds) Privacy Technologies and Policy, Springer International Publishing, Cham, pp 143–160

72. Tøndel IA, Jaatun MG, Meland PH (2008) Security requirements for the rest of us: A survey. IEEE Software 25(1):20–27, DOI 10.1109/MS.2008.19, URL https://doi.org/10.1109/MS.2008.19
73. Tsohou A, Magkos M, Mouratidis H, Chrysoloras G, Piras L, Pavlidis M, Debussche J, Rotoloni M, Crespo BG (2019) Privacy, security, legal and technology acceptance requirements for a GDPR compliance platform. In: Computer Security - ESORICS 2019 International Workshops, CyberICPS, SECPRE, SPOSE, and ADIoT, Luxembourg City, Luxembourg, September 26-27, 2019 Revised Selected Papers, Springer, https://dblp.org/rec/conf/esorics/TsohouMMCPPDRC19.bib, pp 204–223, DOI https://doi.org/10.1007/978-3-030-42048-2_14, URL https://doi.org/10.1007/978-3-030-42048-2_14
74. Tsohou A, Magkos E, Mouratidis H, Chrysoloras G, Piras L, Pavlidis M, Debussche J, Rotoloni M, Crespo BG (2020) Privacy, security, legal and technology acceptance elicited and consolidated requirements for a GDPR compliance platform. Inf Comput Secur 28(4):531–553
75. Veseli F, Serna-Olvera J, Pulls T, Rannenberg K (2019) Engineering privacy by design: lessons from the design and implementation of an identity wallet platform. In: Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing, SAC 2019, Limassol, Cyprus, April 8-12, 2019, ACM, https://dblp.org/rec/conf/sac/VeseliSPR19.bib, pp 1475–1483, DOI 10.1145/3297280.3297429, URL https://doi.org/10.1145/3297280.3297429
76. Vilela J, Silva C, Castro J, Martins LEG, Gorschek T (2019) Sarssi*: a safety requirements specification method based on stamp/stpa and i* language. In: Anais do I Brazilian Workshop on Large-scale Critical Systems, SBC, Porto Alegre, RS, Brasil, pp 17–24, DOI 10.5753/bware.2019.7504, URL https://sol.sbc.org.br/index.php/bware/article/view/7504
77. Yu E, Cysneiros L (2002) Designing for privacy and other competing requirements. In: 2nd Symposium on Requirements Engineering for Information Security (SREIS'02), Raleigh, North Carolina, Citeseer, http://citeseerx.ist.psu.edu/, pp 15–16