Making Privacy Usable: Bridging Privacy Research and Practice Through Guidelines

Abstract

This work presents the User Privacy Communication (UPC) Catalogue, a structured collection of research-based guidelines designed to bridge the gap between privacy research and privacy-aware interaction design in personal data-driven systems. The catalogue was derived from a systematic mapping study of 127 user-involving studies, in which common problems, proposed solutions, and underlying rationales were qualitatively analysed and synthesised into guidelines that are further mapped to a unified set of privacy attributes and classified within design spaces for privacy notices and privacy choices proposed in prior research. In addition to describing the conceptual and structural design of the catalogue, this paper reports an empirical evaluation conducted in two instances with a total of 92 participants. Participants used the catalogue to analyse diverse digital platforms, identify privacy communication issues, select relevant guidelines, and propose guideline-informed improvements for personal data–driven interfaces. This evaluation enabled the examination of guideline effectiveness in terms of alignment between identified problems, selected guidelines, and proposed solutions, as well as participants' perceptions of guideline relevance, ease of use, and contribution to understanding data protection principles. The results indicate that the UPC Catalogue supports the formulation of concrete improvement proposals grounded in prior user-centred research, and serves as a practical resource to foster critical reflection and more informed system design decisions regarding personal data–driven interactions.

Keywords:
Privacy Communication, Usable Privacy, Privacy by Design,
Human-Computer Interaction, User-Centred Design, Design Guidelines

1. Guidelines' supporting research

The complete list of references from the original systematic mapping study (SMS) [1] is available online as supplementary material on Zenodo[1]. This appendix reports the subset of 127 studies selected for the present work, all of which involved users at some stage of the research. To preserve traceability with the original SMS corpus of 231 studies, the selected papers retain their original Paper IDs. Tables 1 and 2 list the Paper IDs cited in the main text along with their titles and the corresponding guidelines they support.

[1] https://github.com/upc-review

Table 1: List of Selected Papers - Part 1

Paper ID	Title	Paper ID	Title
P1	A "Nutrition Label" for Privacy (GD2) [2]	P4	A Framework for Computing the Privacy Scores of Users in Online Social Networks (GD21) [3]
P7	A human-centered artificial intelligence approach for privacy protection of elderly App users in smart cities (GD10) [4]	P8	A joint sharing approach for online privacy preservation (GD18) [5]
P11	A Machine-Learning Based Approach to Privacy-Aware Information-Sharing in Mobile Social Networks (GD14) [6]	P15	A Privacy Settings Prediction Model for Textual Posts on Social Networks (GD14) [7]
P18	A recommendation approach for user privacy preferences in the fitness domain (GD14) [8]	P20	A Semi-supervised Approach to Measuring User Privacy in Online Social Networks (GD21) [9]
P25	A Visualization Interface to Improve the Transparency of Collected Personal Data on the Internet (GD24) [10]	P26	Addressing The Privacy Paradox through Personalized Privacy Notifications (GD7, GD19) [11]
P33	An evaluation of three designs to engage users when providing their consent on smartphones (GD12) [12]	P35	Android User Privacy Preserving Through Crowdsourcing (GD8) [13]
P36	AppMonitor: restricting information leakage to third-party applications (GD15) [14]	P38	Aquilis: Using Contextual Integrity for Privacy Protection on Mobile Devices (GD19) [15]
P40	Automated and Personalized Privacy Policy Extraction Under GDPR Consideration (GD4) [16]	P42	Automated privacy negotiations with preference uncertainty (GD14) [17]
P43	Automated Privacy Preferences for Smart Home Data Sharing Using Personal Data Stores (GD14) [18]	P47	Automating Contextual Privacy Policies: Design and Evaluation of a Production Tool for Digital Consumer Privacy Awareness. (GD4) [19]
P48	Autonomous Permission Recommendation (GD8) [20]	P49	Better the Devil You Know: Exposing the Data Sharing Practices of Smartphone Apps (GD7) [21]
P50	Calculation of account reachability risk for users having multiple SNS accounts from user's profile and regional information (GD21) [22]	P51	Cardea: Context–Aware Visual Privacy Protection for Photo Taking and Sharing (GD17) [23]
P53	Collaborative privacy management (GD5) [24]	P55	Configuring Audience-Oriented Privacy Policies (GD15) [25]
P56	Consent recommender system: A case study on LinkedIn settings (GD14) [26]	P58	Contextualizing Privacy Decisions for Better Prediction (and Protection) (GD6, GD8) [27]
P60	CoPE: Enabling collaborative privacy management in online social networks (GD18) [28]	P61	DaPIS: An Ontology-Based Data Protection Icon Set (GD3) [29]
P62	Data Dashboard: Exploring Centralization and Customization in Personal Data Curation (GD25) [30]	P63	Data-Driven Privacy Indicators (GD7) [31]
P65	Default privacy setting prediction by grouping user's attributes and settings preferences (GD14) [32]	P66	Design and Implementation of a CBR-based Privacy Agent (GD14) [33]
P67	Designing a GDPR-compliant and usable privacy dashboard (GD25) [34]	P68	Designing privacy indicators for smartphone app markets: A new perspective on the nature of privacy risks of apps (GD7, GD19) [35]
P70	Detecting and resolving privacy conflicts for collaborative data sharing in online social networks (GD18) [36]	P71	Does this App Really Need My Location?: Context-Aware Privacy Management for Smartphones (GD6) [37]
P72	ELVIRA: An Explainable Agent for Value and Utility-Driven Multiuser Privacy (GD18) [38]	P74	Enhancing privacy through the visual design of privacy notices: Exploring the interplay of curiosity, control and affect (GD2) [39]
P75	Enhancing the privacy risk awareness of teenagers in online social networks through soft-paternalism mechanisms (GD20) [40]	P77	Evaluation of the reliability of using the prototype PPMARK - A tool to support the computer human interaction in readings the privacy policies - Using the GQM and TAM models (GD4) [41]
P78	Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing (GD23) [42]	P80	Extending Layered Privacy Language to Support Privacy Icons for a Personal Privacy Policy User Interface (GD3) [43]
P81	Eyeing Your Exposure: Quantifying and Controlling Information Sharing for Improved Privacy (GD15) [44]	P82	Finding a Choice in a Haystack: Automatic Extraction of Opt-Out Statements from Privacy Policy Text (GD13) [45]
P83	Follow My Recommendations: A Personalized Privacy Assistant for Mobile App Permissions (GD8) [46]	P85	From Design Requirements to Effective Privacy Notifications: Empowering Users of Online Services to Make Informed Decisions (GD25) [47]
P86	From Tag to Protect: A Tag-Driven Policy Recommender System for Image Sharing (GD14) [48]	P87	Have You been Properly Notified? Automatic Compliance Analysis of Privacy Policy Text with GDPR Article 13 (GD5) [49]
P88	Helping john to make informed decisions on using social login (GD12) [50]	P90	HideMe: Privacy-Preserving Photo Sharing on Social Networks (GD17) [51]
P91	If You Can't Beat Them, Join Them: A Usability Approach to Interdependent Privacy in Cloud Apps (GD16) [52]	P95	Increasing Service Users' Privacy Awareness by Introducing On-Line Interactive Privacy Features (GD21) [53]
P96	Information flows as a permission mechanism (GD7) [54]	P97	Interaction and Visualization Design for User Privacy Interface on Online Social Networks (GD20, GD21) [55]
P98	Introducing privacy threats from ad libraries to android users through privacy granules (GD7, GD19, GD23) [56]	P102	Knapsack graph-based privacy checking for smart environments (GD14) [57]
P103	KnIGHT: Mapping Privacy Policies to GDPR (GD4) [58]	P108	Location privacy protection for smartphone users (GD6) [59]
P111	Moving beyond set-it-and-forget-it privacy settings on social media (GD14) [60]	P112	Multi-view permission risk notification for smartphone system (GD21, GD22) [61]
P113	Multiparty access control for online social networks: Model and mechanisms (GD18) [62]	P115	No technical understanding required: Helping users make informed choices about access to their personal data (GD7, GD23) [63]
P117	Nudging the user with privacy indicator: a study on the app selection behavior of the user (GD7, GD19) [64]	P118	On a (Per)Mission: Building Privacy Into the App Marketplace (GD6, GD7) [65]
P119	OnLITE: On-line Label for IoT Transparency Enhancement (GD5) [66]	P120	PACMAN: Personal Agent for Access Control in Social Media (GD14) [67]

Table 2: List of Selected Papers - Part 2

Paper ID	Title	Paper ID	Title
P122	PARA: Privacy Management and Control in Emerging IoT Ecosystems using Augmented Reality (GD10) [68]	P123	Partial Consent: A Study on User Preference for Informed Consent (GD6) [69]
P124	Pattern-based incorporation of privacy preferences into privacy policies: negotiating the conflicting needs of service providers and end-users (GD13) [70]	P125	PDVLoc: A Personal Data Vault for Controlled Location Data Sharing (GD11) [71]
P133	Polisis: Automated analysis and presentation of privacy policies using deep learning (GD4) [72]	P136	Preventative Nudges: Introducing Risk Cues for Supporting Online Self-Disclosure Decisions (GD20) [73]
P137	PriGuardTool: A web-based tool to detect privacy violations semantically (GD21) [74]	P139	PriMe: Human-centric Privacy Measurement based on User Preferences towards Data Sharing in Mobile Participatory Sensing Systems (GD21) [75]
P140	PriSEC: A privacy settings enforcement controller (GD13) [76]	P141	Privacy as part of the app decision-making process (GD7, GD23) [77]
P142	Privacy Care: A Tangible Interaction Framework for Privacy Management (GD10) [78]	P143	Privacy CURE: Consent Comprehension Made Easy (GD1) [79]
P149	Privacy Negotiation Mechanism in Internet of Things Environments (GD14) [80]	P150	Privacy Pal: Improving Permission Safety Awareness of Third Party Applications in Online Social Networks (GD7, GD19, GD23) [81]
P151	Privacy policies for shared content in social network sites (GD18) [82]	P152	Privacy Policy Inference of User-Uploaded Images on Content Sharing Sites (GD14) [83]
P154	Privacy preference modeling and prediction in a simulated campuswide IoT environment (GD14) [84]	P155	Privacy Protection Based Privacy Conflict Detection and Solution in Online Social Networks (GD18) [85]
P156	Privacy rating: a user-centered approach for visualizing data handling practices of online services (GD2) [86]	P159	Privacy Settings Recommender for Online Social Network (GD14) [87]
P160	Privacy theory in practice: designing a user interface for managing location privacy on mobile devices (GD6) [88]	P162	Privacy-Aware Personal Data Storage (P-PDS): Learning how to Protect User Privacy from External Applications (GD11) [89]
P169	PrivacyPrimer: Towards Privacy-Preserving Episodic Memory Support for Older Adults (GD10) [90]	P173	PriView – Exploring Visualisations to Support Users' Privacy Awareness (GD21) [91]
P176	Quality of Private Information (QoPI) model for effective representation and prediction of privacy controls in mobile computing (GD8) [92]	P179	Recommendations for a smart toy parental control tool (GD9) [93]
P180	REMIND: Risk Estimation Mechanism for Images in Network Distribution (GD17, GD21) [94]	P181	Resolving Multi-Party Privacy Conflicts in Social Media (GD18) [95]
P183	Scoring Users' Privacy Disclosure Across Multiple Online Social Networks (GD21) [96]	P184	Seeing is believing: Towards interactive visual exploration of data privacy in federated learning (GD21) [97]
P186	Semantic-based privacy settings negotiation and management (GD11) [98]	P187	SmarPer: Context-Aware and Automatic Runtime-Permissions for Mobile Devices (GD8) [99]
P188	Smart Data Agent for Preserving Location Privacy (GD8) [100]	P189	Smart toys and children's privacy: Usable privacy policy insights from a card sorting experiment (GD9) [101]
P191	Styx: Privacy risk communication for the Android smartphone platform based on apps' data-access behavior patterns (GD21, GD23) [102]	P193	Textured agreements: re-envisioning electronic consent (GD2) [103]
P194	The Feasibility of Dynamically Granted Permissions: Aligning Mobile Privacy with User Preferences (GD8) [104]	P196	The privacy badge: A privacy-awareness user interface for small devices (GD21) [105]
P197	TLDR: Deep Learning-Based Automated Privacy Policy Annotation with Key Policy Highlights (GD4) [106]	P198	Toward an Approach to Privacy Notices in IoT (GD4) [107]
P203	Towards a Visual Privacy Advisor: Understanding and Predicting Privacy Risks in Images (GD14) [108]	P204	Towards Automated Content-based Photo Privacy Control in User-Centered Social Networks (GD20) [109]
P206	Towards Consensus-Based Group Decision Making for Co-Owned Data Sharing in Online Social Networks (GD18) [110]	P207	Towards displaying privacy information with icons (GD3) [111]
P208	Towards PII-based multiparty access control for photo sharing in Online Social Networks (GD17) [112]	P211	Towards usable privacy policy display & management (GD1) [113]
P212	Trend Analysis and Recommendation of Users' Privacy Settings on Social Networking Services (GD14) [114]	P217	Unwinding Ariadne's Identity Thread: Privacy Risks with Fitness Trackers and Online Social Networks (GD21) [115]
P218	User-Centric Privacy for Identity Federations Based on a Recommendation System (GD14) [116]	P219	User-Controllable Learning of Security and Privacy Policies (GD14) [117]
P220	User-friendly privacy-preserving photo sharing on online social networks (GD15) [118]	P221	VeilMe: An interactive visualization tool for privacy configuration of using personality traits (GD14, GD15) [119]
P222	Visual configuration of mobile privacy policies (GD6) [120]	P223	Visual Interactive Privacy Policy: The Better Choice? (GD1, GD2) [121]
P224	Visualizing Exports of Personal Data by Exercising the Right of Data Portability in the Data Track - Are People Ready for This? (GD24) [122]	P225	Visualizing Past Personal Data Disclosures (GD24) [123]
P226	Visualizing privacy risks of mobile applications through a privacy meter (GD23) [124]	P227	Visualizing social roles - Design and evaluation of a bird's-eye view of social network privacy settings (GD25) [125]
P228	What About My Privacy? Helping Users Understand Online Privacy Policies (GD4) [126]	P231	When Privacy Meets Usability: Unobtrusive Privacy Permission Recommendation System for Mobile Apps Based on Crowdsourcing (GD8) [127]
P232 [1]	Who is Visible: Resolving Access Policy Conflicts in Online Social Networks (GD18) [128]		

[1] Paper P175 was removed after the initial indexing of the SMS corpus. To preserve identifier consistency and avoid cascading renumbering errors, subsequent Paper IDs were left unchanged, resulting in the presence of P232 within a corpus of 231 selected papers.

References

[1] Anonymous, Details omitted for double-anonymised reviewing (2025).

[2] P. G. Kelley, J. Bresee, L. F. Cranor, R. W. Reeder, A "nutrition label" for privacy, in: Proceedings of the 5th Symposium on Usable Privacy and Security, SOUPS '09, Association for Computing Machinery, New York, NY, USA, 2009. doi:10.1145/1572532.1572538.
URL https://doi.org/10.1145/1572532.1572538

[3] K. Liu, E. Terzi, A framework for computing the privacy scores of users in online social networks, ACM Transactions on Knowledge Discovery from Data (TKDD) 5 (1) (Dec. 2010). doi:10.1145/1870096.1870102.
URL https://doi.org/10.1145/1870096.1870102

[4] H. Elahi, A. Castiglione, G. Wang, O. Geman, A human-centered artificial intelligence approach for privacy protection of elderly app users in smart cities, Neurocomputing 444 (2021) 189–202. doi:10.1016/j.neucom.2020.06.149.
URL https://doi.org/10.1016/j.neucom.2020.06.149

[5] T. Muhammad, A. Ahmad, A joint sharing approach for online privacy preservation, World Wide Web 24 (3) (2021) 895–924. doi:10.1007/s11280-021-00876-5.
URL https://doi.org/10.1007/s11280-021-00876-5

[6] I. Bilogrevic, K. Huguenin, B. Agir, M. Jadliwala, M. Gazaki, J.-P. Hubaux, A machine-learning based approach to privacy-aware information-sharing in mobile social networks, Pervasive and Mobile Computing 25 (2016) 125–142. doi:10.1016/j.pmcj.2015.01.006.
URL https://doi.org/10.1016/j.pmcj.2015.01.006

[7] L. Chen, M. Xu, X. Yang, N. Zheng, Y. Wu, J. Xu, T. Qiao, H. Liu, A privacy settings prediction model for textual posts on social networks, in: International Conference on Collaborative Computing: Networking, Applications and Worksharing, Springer, Cham, 2017, pp. 578–588. doi:10.1007/978-3-030-00916-8_53.
URL https://doi.org/10.1007/978-3-030-00916-8_53

[8] O. R. Sanchez, I. Torre, Y. He, B. P. Knijnenburg, A recommendation approach for user privacy preferences in the fitness domain, User Modeling and User-Adapted Interaction 30 (3) (2020) 513–565. doi:10.1007/s11257-019-09246-3.
URL https://doi.org/10.1007/s11257-019-09246-3

[9] R. G. Pensa, G. D. Blasi, A semi-supervised approach to measuring user privacy in online social networks, in: International Conference on Discovery Science, Springer, Cham, 2016, pp. 392–407. doi:10.1007/978-3-319-46307-0_25.
URL https://doi.org/doi={10.1007/978-3-319-46307-0_25}

[10] M. Schufrin, S. L. Reynolds, A. Kuijper, J. Kohlhammer, A visualization interface to improve the transparency of collected personal data on the internet, IEEE Transactions on Visualization and Computer Graphics 27 (2) (2021) 1840–1849. doi:10.1109/TVCG.2020.3028946.
URL https://doi.org/10.1109/TVCG.2020.3028946

[11] C. B. Jackson, Y. Wang, Addressing the privacy paradox through personalized privacy notifications, Proc. ACM Interact. Mob. Wearable Ubiquitous Technol. 2 (2) (Jul. 2018). doi:10.1145/3214271.
URL https://doi.org/10.1145/3214271

[12] D. Lindegren, F. Karegar, B. Kane, J. S. Pettersson, An evaluation of three designs to engage users when providing their consent on smartphones, Behaviour & Information Technology 40 (4) (2021) 398–414.
URL https://doi.org/10.1080/0144929X.2019.1697898

[13] B. Rashidi, C. Fung, A. Nguyen, T. Vu, E. Bertino, Android user privacy preserving through crowdsourcing, IEEE Transactions on Information Forensics and Security 13 (3) (2018) 773–787. doi:10.1109/TIFS.2017.2767019.
URL https://doi.org/10.1109/TIFS.2017.2767019

[14] N. C. Rathore, S. Tripathy, Appmonitor: restricting information leakage to third-party applications, Social Network Analysis and Mining 10 (1) (2020) 1–20.
URL https://doi.org/10.1007/s13278-020-00662-7

[15] A. Kumar, T. Braud, Y. D. Kwon, P. Hui, Aquilis: Using contextual integrity for privacy protection on mobile devices, Proc. ACM Interact. Mob. Wearable Ubiquitous Technol. 4 (4) (Dec. 2020). doi:10.1145/3432205.
URL https://doi.org/10.1145/3432205

[16] C. Chang, H. Li, Y. Zhang, S. Du, H. Cao, H. Zhu, Automated and personalized privacy policy extraction under gdpr consideration, in: International Conference on Wireless Algorithms, Systems, and Applications, Springer, Cham, 2019, pp. 43–54.
URL https://doi.org/10.1007/978-3-030-23597-0_4

[17] D. Filipczuk, T. Baarslag, E. H. Gerding, M. Schraefel, Automated privacy negotiations with preference uncertainty, Autonomous Agents and Multi-Agent Systems 36 (2) (2022) 1–38. doi:10.1007/s10458-022-09579-1.
URL https://doi.org/10.1007/s10458-022-09579-1

[18] Y. Shanmugarasa, H.-y. Paik, S. S. Kanhere, L. Zhu, Automated privacy preferences for smart home data sharing using personal data stores, IEEE Security & Privacy 20 (1) (2022) 12–22. doi:10.1109/MSEC.2021.3106056.
URL https://doi.org/10.1109/MSEC.2021.3106056

[19] M. Windl, N. Henze, A. Schmidt, S. S. Feger, Automating contextual privacy policies: Design and evaluation of a production tool for digital consumer privacy awareness, in: Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems, CHI '22, Association for Computing Machinery, New York, NY, USA, 2022. doi:10.1145/3491102.3517688.
URL https://doi.org/10.1145/3491102.3517688

[20] H. Gao, C. Guo, D. Huang, X. Hou, Y. Wu, J. Xu, Z. He, G. Bai, Autonomous permission recommendation, IEEE Access 8 (2020) 76580–76594. doi:10.1109/ACCESS.2020.2967139.
URL https://doi.org/10.1109/ACCESS.2020.2967139

[21] M. Van Kleek, I. Liccardi, R. Binns, J. Zhao, D. J. Weitzner, N. Shadbolt, Better the devil you know: Exposing the data sharing practices of smartphone apps, in: Proceedings of the 2017 CHI Confer-

ence on Human Factors in Computing Systems, CHI '17, Association for Computing Machinery, New York, NY, USA, 2017, p. 5208–5220. doi:10.1145/3025453.3025556.
URL https://doi.org/10.1145/3025453.3025556

[22] A. Yoshikuni, C. Watanabe, Calculation of account reachability risk for users having multiple sns accounts from user's profile and regional information, International Journal of Web Information Systems 11 (2015). doi:10.1108/IJWIS-03-2014-0010.
URL https://doi.org/10.1108/IJWIS-03-2014-0010

[23] J. Shu, R. Zheng, P. Hui, Cardea: context-aware visual privacy protection for photo taking and sharing, in: Proceedings of the 9th ACM Multimedia Systems Conference, MMSys '18, Association for Computing Machinery, New York, NY, USA, 2018, p. 304–315. doi:10.1145/3204949.3204973.
URL https://doi.org/10.1145/3204949.3204973

[24] J. Kolter, T. Kernchen, G. Pernul, Collaborative privacy management, Computers & Security 29 (5) (2010) 580–591.
URL https://doi.org/10.1016/j.cose.2009.12.007

[25] J. Watson, M. Whitney, H. R. Lipford, Configuring audience-oriented privacy policies, in: Proceedings of the 2nd ACM Workshop on Assurable and Usable Security Configuration, SafeConfig '09, Association for Computing Machinery, New York, NY, USA, 2009, p. 71–78. doi:10.1145/1655062.1655076.
URL https://doi.org/10.1145/1655062.1655076

[26] K. Rosni, M. Shukla, V. Banahatti, S. Lodha, Consent recommender system: A case study on linkedin settings, in: Proceedings of the PAL: Privacy-Enhancing Artificial Intelligence and Language Technologies, CEUR Workshop Proceedings, Palo Alto, USA, 2019.
URL https://ceur-ws.org/Vol-2335/1st_PAL_paper_12.pdf

[27] P. Wijesekera, J. Reardon, I. Reyes, L. Tsai, J.-W. Chen, N. Good, D. Wagner, K. Beznosov, S. Egelman, Contextualizing privacy decisions for better prediction (and protection), in: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, CHI '18, Association for Computing Machinery, New York, NY, USA, 2018,

p. 1–13. doi:10.1145/3173574.3173842.
URL https://doi.org/10.1145/3173574.3173842

[28] A. C. Squicciarini, H. Xu, X. Zhang, Cope: Enabling collaborative privacy management in online social networks, Journal of the American Society for Information Science and Technology 62 (3) (2011) 521–534.
URL https://doi.org/10.1002/asi.21473

[29] A. Rossi, M. Palmirani, Dapis: An ontology-based data protection icon set, Knowledge of the Law in the Big Data Age 317 (2019) 181.
URL https://ebooks.iospress.nl/doi/10.3233/FAIA190020

[30] F. Vitale, J. Chen, W. Odom, J. McGrenere, Data dashboard: Exploring centralization and customization in personal data curation, in: Proceedings of the 2020 ACM Designing Interactive Systems Conference, DIS '20, Association for Computing Machinery, New York, NY, USA, 2020, p. 311–326. doi:10.1145/3357236.3395457.
URL https://doi.org/10.1145/3357236.3395457

[31] H. Harkous, R. Rahman, K. Aberer, Data-Driven privacy indicators, in: Twelfth Symposium on Usable Privacy and Security (SOUPS'2016), USENIX Association, Denver, CO, 2016, pp. 1–10.
URL https://www.usenix.org/conference/soups2016/workshop-program/wpi/presentation/harkous

[32] T. Nakamura, W. B. Tesfay, S. Kiyomoto, J. Serna, Default privacy setting prediction by grouping user's attributes and settings preferences, in: Data privacy management, cryptocurrencies and blockchain technology, Springer, Cham, 2017, pp. 107–123. doi:10.1007/978-3-319-67816-0_7.
URL https://doi.org/10.1007/978-3-319-67816-0_7

[33] K. Bernsmed, I. A. Tøndel, Å. A. Nyre, Design and implementation of a cbr-based privacy agent, in: 2012 Seventh International Conference on Availability, Reliability and Security, IEEE, New York, NY, USA, 2012, pp. 317–326. doi:10.1109/ARES.2012.60.
URL https://doi.org/10.1109/ARES.2012.60

[34] P. Raschke, A. Küpper, O. Drozd, S. Kirrane, Designing a gdpr-compliant and usable privacy dashboard, in: IFIP international summer school on privacy and identity management, Springer, Cham, 2017,

pp. 221–236. doi:10.1007/978-3-319-92925-5_14.
URL https://doi.org/10.1007/978-3-319-92925-5_14

[35] G. Bal, Designing privacy indicators for smartphone app markets: A new perspective on the nature of privacy risks of apps, in: Proceedings of the 20th Americas Conference on Information Systems, AMCIS 2014, ssociation for Information Systems, Georgia, USA, 2014, p. 12.
URL https://aisel.aisnet.org/amcis2014/MobileComputing/GeneralPresentations/6

[36] H. Hu, G.-J. Ahn, J. Jorgensen, Detecting and resolving privacy conflicts for collaborative data sharing in online social networks, in: Proceedings of the 27th Annual Computer Security Applications Conference, ACSAC '11, Association for Computing Machinery, New York, NY, USA, 2011, p. 103–112. doi:10.1145/2076732.2076747.
URL https://doi.org/10.1145/2076732.2076747

[37] S. Chitkara, N. Gothoskar, S. Harish, J. I. Hong, Y. Agarwal, Does this app really need my location? context-aware privacy management for smartphones, in: Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, Vol. 1, Association for Computing Machinery, New York, NY, USA, 2017. doi:10.1145/3132029.
URL https://doi.org/10.1145/3132029

[38] F. Mosca, J. M. Such, Elvira: An explainable agent for value and utility-driven multiuser privacy, in: Proceedings of the 20th International Conference on Autonomous Agents and MultiAgent Systems, AAMAS '21, International Foundation for Autonomous Agents and Multiagent Systems, Richland, SC, 2021, p. 916–924.
URL https://dl.acm.org/doi/10.5555/3463952.3464061

[39] A. Kitkowska, M. Warner, Y. Shulman, E. Wästlund, L. A. Martucci, Enhancing privacy through the visual design of privacy notices: Exploring the interplay of curiosity, control and affect, in: Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020), USENIX Association, Berkeley, CA, USA, 2020, pp. 437–456.
URL https://www.usenix.org/conference/soups2020/presentation/kitkowska

[40] J. Alemany, E. Del Val, J. Alberola, A. García-Fornes, Enhancing the privacy risk awareness of teenagers in online social networks through soft-paternalism mechanisms, International Journal of Human-Computer Studies 129 (2019) 27–40. doi:10.1016/j.ijhcs.2019.03.008.
URL https://doi.org/10.1016/j.ijhcs.2019.03.008

[41] D. R. G. Pontes, S. D. Zorzo, J. S. M. Mello, Evaluation of the reliability of using the prototype ppmark-a tool to support the computer human interaction in readings the privacy policies-using the gqm and tam models., in: AMCIS 2017 Proceedings., Association for Information Systems, Boston, USA, 2017.
URL https://aisel.aisnet.org/amcis2017/InformationSystems/Presentations/22

[42] J. Lin, S. Amini, J. I. Hong, N. Sadeh, J. Lindqvist, J. Zhang, Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing, in: Proceedings of the 2012 ACM Conference on Ubiquitous Computing, UbiComp '12, Association for Computing Machinery, New York, NY, USA, 2012, p. 501–510. doi:10.1145/2370216.2370290.
URL https://doi.org/10.1145/2370216.2370290

[43] A. Gerl, Extending layered privacy language to support privacy icons for a personal privacy policy user interface, in: Proceedings of the 32nd International BCS Human Computer Interaction Conference 32, ScienceOpen, Belfast United Kingdom, 2018, pp. 1–5.

[44] R. Schlegel, A. Kapadia, A. J. Lee, Eyeing your exposure: quantifying and controlling information sharing for improved privacy, in: Proceedings of the Seventh Symposium on Usable Privacy and Security, SOUPS '11, Association for Computing Machinery, New York, NY, USA, 2011. doi:10.1145/2078827.2078846.
URL https://doi.org/10.1145/2078827.2078846

[45] V. Bannihatti Kumar, R. Iyengar, N. Nisal, Y. Feng, H. Habib, P. Story, S. Cherivirala, M. Hagan, L. Cranor, S. Wilson, F. Schaub, N. Sadeh, Finding a choice in a haystack: Automatic extraction of opt-out statements from privacy policy text, in: Proceedings of The Web Conference

2020, WWW '20, Association for Computing Machinery, New York, NY, USA, 2020, p. 1943–1954. doi:10.1145/3366423.3380262.
URL https://doi.org/10.1145/3366423.3380262

[46] B. Liu, M. S. Andersen, F. Schaub, H. Almuhimedi, S. A. Zhang, N. Sadeh, Y. Agarwal, A. Acquisti, Follow my recommendations: A personalized privacy assistant for mobile app permissions, in: Twelfth Symposium on Usable Privacy and Security, USENIX Association, Berkeley, CA, USA, 2016, pp. 27–41.
URL https://www.usenix.org/conference/soups2016/technical-sessions/presentation/liu

[47] P. Murmann, F. Karegar, From design requirements to effective privacy notifications: Empowering users of online services to make informed decisions, International Journal of Human–Computer Interaction 37 (19) (2021) 1823–1848.
URL https://doi.org/10.1080/10447318.2021.1913859

[48] A. C. Squicciarini, A. Novelli, D. Lin, C. Caragea, H. Zhong, From tag to protect: A tag-driven policy recommender system for image sharing, in: 2017 15th Annual Conference on Privacy, Security and Trust (PST), IEEE, New York, NY, USA, 2017, pp. 337–33709. doi:10.1109/PST.2017.00047.
URL https://doi.org/10.1109/PST.2017.00047

[49] S. Liu, B. Zhao, R. Guo, G. Meng, F. Zhang, M. Zhang, Have you been properly notified? automatic compliance analysis of privacy policy text with gdpr article 13, in: Proceedings of the Web Conference 2021, WWW '21, Association for Computing Machinery, New York, NY, USA, 2021, p. 2154–2164. doi:10.1145/3442381.3450022.
URL https://doi.org/10.1145/3442381.3450022

[50] F. Karegar, N. Gerber, M. Volkamer, S. Fischer-Hübner, Helping john to make informed decisions on using social login, in: Proceedings of the 33rd Annual ACM Symposium on Applied Computing, SAC '18, Association for Computing Machinery, New York, NY, USA, 2018, p. 1165–1174. doi:10.1145/3167132.3167259.
URL https://doi.org/10.1145/3167132.3167259

[51] F. Li, Z. Sun, A. Li, B. Niu, H. Li, G. Cao, Hideme: Privacy-preserving photo sharing on social networks, in: IEEE INFOCOM 2019-IEEE Conference on Computer Communications, IEEE, New York, NY, USA, 2019, pp. 154–162. `doi:10.1109/INFOCOM.2019.8737466`.
URL `https://doi.org/10.1109/INFOCOM.2019.8737466`

[52] H. Harkous, K. Aberer, "if you can't beat them, join them": A usability approach to interdependent privacy in cloud apps, in: Proceedings of the Seventh ACM on Conference on Data and Application Security and Privacy, CODASPY '17, Association for Computing Machinery, New York, NY, USA, 2017, p. 127–138. `doi:10.1145/3029806.3029837`.
URL `https://doi.org/10.1145/3029806.3029837`

[53] E. Kani-Zabihi, M. Helmhout, Increasing service users' privacy awareness by introducing on-line interactive privacy features, in: P. Laud (Ed.), Information Security Technology for Applications, Springer Berlin Heidelberg, Berlin, Heidelberg, 2012, pp. 131–148. `doi:10.1007/978-3-642-29615-4_10`.
URL `https://doi.org/10.1007/978-3-642-29615-4_10`

[54] F. Shen, N. Vishnubhotla, C. Todarka, M. Arora, B. Dhandapani, E. J. Lehner, S. Y. Ko, L. Ziarek, Information flows as a permission mechanism, in: Proceedings of the 29th ACM/IEEE International Conference on Automated Software Engineering, ASE '14, Association for Computing Machinery, New York, NY, USA, 2014, p. 515–526. `doi:10.1145/2642937.2643018`.
URL `https://doi.org/10.1145/2642937.2643018`

[55] T. T. Dang, K. T. Dang, J. Küng, Interaction and visualization design for user privacy interface on online social networks, SN Computer Science 1 (5) (2020) 1–12. `doi:10.1007/s42979-020-00314-9`.
URL `https://doi.org/10.1007/s42979-020-00314-9`

[56] A. Paturi, P. G. Kelley, S. Mazumdar, Introducing privacy threats from ad libraries to android users through privacy granules, in: Proceedings of NDSS Workshop on Usable Security (USEC'15), Vol. 1, Internet Society, San Diego, CA, USA, 2015, pp. 2–1.
URL `http://dx.doi.org/10.14722/usec.2015.23008`

[57] Z. Alom, B. C. Singh, Z. Aung, M. A. Azim, Knapsack graph-based privacy checking for smart environments, Computers & Security 105 (2021) 102240. doi:10.1016/j.cose.2021.102240.
URL https://doi.org/10.1016/j.cose.2021.102240

[58] N. Mousavi Nejad, S. Scerri, J. Lehmann, Knight: Mapping privacy policies to gdpr, in: European Knowledge Acquisition Workshop, Springer, Cham, 2018, pp. 258–272. doi:10.1007/978-3-030-03667-6_17.
URL 10.1007/978-3-030-03667-6_17

[59] K. Fawaz, K. G. Shin, Location privacy protection for smartphone users, in: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, CCS '14, Association for Computing Machinery, New York, NY, USA, 2014, p. 239–250. doi:10.1145/2660267.2660270.
URL https://doi.org/10.1145/2660267.2660270

[60] M. Mondal, G. S. Yilmaz, N. Hirsch, M. T. Khan, M. Tang, C. Tran, C. Kanich, B. Ur, E. Zheleva, Moving beyond set-it-and-forget-it privacy settings on social media, in: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, CCS '19, Association for Computing Machinery, New York, NY, USA, 2019, p. 991–1008. doi:10.1145/3319535.3354202.
URL https://doi.org/10.1145/3319535.3354202

[61] C. J. Fung, B. Rashidi, V. G. Motti, Multi-view permission risk notification for smartphone system., J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl. 10 (1) (2019) 42–57. doi:10.22667/JOWUA.2019.03.31.042.
URL https://doi.org/10.22667/JOWUA.2019.03.31.042

[62] H. Hu, G.-J. Ahn, J. Jorgensen, Multiparty access control for online social networks: Model and mechanisms, IEEE Transactions on Knowledge and Data Engineering 25 (7) (2013) 1614–1627. doi:10.1109/TKDE.2012.97.
URL https://doi.org/10.1109/TKDE.2012.97

[63] I. Liccardi, J. Pato, D. J. Weitzner, H. Abelson, D. De Roure, No technical understanding required: helping users make informed choices

about access to their personal data, in: Proceedings of the 11th International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, MOBIQUITOUS '14, ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), Brussels, BEL, 2014, p. 140–150. doi:10.4108/icst.mobiquitous.2014.258066.
URL https://doi.org/10.4108/icst.mobiquitous.2014.258066

[64] S. Bock, N. Momen, Nudging the user with privacy indicator: A study on the app selection behavior of the user, in: Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society, NordiCHI '20, Association for Computing Machinery, New York, NY, USA, 2020. doi:10.1145/3419249.3420111.
URL https://doi.org/10.1145/3419249.3420111

[65] H. Quay-de la Vallee, P. Selby, S. Krishnamurthi, On a (per)mission: Building privacy into the app marketplace, in: Proceedings of the 6th Workshop on Security and Privacy in Smartphones and Mobile Devices, SPSM '16, Association for Computing Machinery, New York, NY, USA, 2016, p. 63–72. doi:10.1145/2994459.2994466.
URL https://doi.org/10.1145/2994459.2994466

[66] A. Railean, D. Reinhardt, Onlite: On-line label for iot transparency enhancement, in: Nordic Conference on Secure IT Systems, Springer, Cham, 2020, pp. 229–245. doi:10.1007/978-3-030-70852-8_14.
URL https://doi.org/10.1007/978-3-030-70852-8_14

[67] G. Misra, J. M. Such, Pacman: Personal agent for access control in social media, IEEE Internet Computing 21 (6) (2017) 18–26. doi:10.1109/MIC.2017.4180831.
URL https://doi.org/10.1109/MIC.2017.4180831

[68] C. Bermejo Fernandez, L. H. Lee, P. Nurmi, P. Hui, Para: Privacy management and control in emerging iot ecosystems using augmented reality, in: Proceedings of the 2021 International Conference on Multimodal Interaction, ICMI '21, Association for Computing Machinery, New York, NY, USA, 2021, p. 478–486. doi:10.1145/3462244.3479885.
URL https://doi.org/10.1145/3462244.3479885

[69] S. Bock, A. F. Chowdhury, N. Momen, Partial consent: A study on user preference for informed consent, in: C. Stephanidis, M. M. Soares, E. Rosenzweig, A. Marcus, S. Yamamoto, H. Mori, P.-L. P. Rau, G. Meiselwitz, X. Fang, A. Moallem (Eds.), HCI International 2021 - Late Breaking Papers: Design and User Experience, Springer International Publishing, Cham, 2021, pp. 198–216. doi:10.1007/978-3-030-90238-4_15.
URL https://doi.org/10.1007/978-3-030-90238-4_15

[70] N. G. Mohammadi, J. Pampus, M. Heisel, Pattern-based incorporation of privacy preferences into privacy policies: negotiating the conflicting needs of service providers and end-users, in: Proceedings of the 24th European Conference on Pattern Languages of Programs, EuroPLop '19, Association for Computing Machinery, New York, NY, USA, 2019. doi:10.1145/3361149.3361154.
URL https://doi.org/10.1145/3361149.3361154

[71] M. Y. Mun, D. H. Kim, K. Shilton, D. Estrin, M. Hansen, R. Govindan, Pdvloc: A personal data vault for controlled location data sharing, ACM Trans. Sen. Netw. 10 (4) (Jun. 2014). doi:10.1145/2523820.
URL https://doi.org/10.1145/2523820

[72] H. Harkous, K. Fawaz, R. Lebret, F. Schaub, K. G. Shin, K. Aberer, Polisis: Automated analysis and presentation of privacy policies using deep learning, in: 27th USENIX Security Symposium (USENIX Security 18), USENIX, Baltimore MD USA, 2018, pp. 531–548.
URL https://www.usenix.org/conference/usenixsecurity18/presentation/harkous

[73] N. E. Díaz Ferreyra, T. Kroll, E. Aïmeur, S. Stieglitz, M. Heisel, Preventative nudges: Introducing risk cues for supporting online self-disclosure decisions, Information (Switzerland) 11 (8) (2020). doi:10.3390/INFO11080399.
URL https://doi.org/10.3390/INFO11080399

[74] N. Kökciyan, P. Yolum, Priguardtool: A web-based tool to detect privacy violations semantically, in: International Workshop on Engineering Multi-Agent Systems, Springer, Cham, 2016, pp. 81–98. doi:10.1007/978-3-319-50983-9_5.
URL https://doi.org/10.1007/978-3-319-50983-9_5

[75] R. Liu, J. Cao, S. VanSyckel, W. Gao, Prime: Human-centric privacy measurement based on user preferences towards data sharing in mobile participatory sensing systems, in: 2016 IEEE International Conference on Pervasive Computing and Communications (PerCom), IEEE, New York, NY, USA, 2016, pp. 1–8. doi:10.1109/PERCOM.2016.7456518. URL https://doi.org/10.1109/PERCOM.2016.7456518

[76] R. Khandelwal, T. Linden, H. Harkous, K. Fawaz, PriSEC: A privacy settings enforcement controller, in: 30th USENIX Security Symposium (USENIX Security 21), USENIX Association, Berkeley, CA, USA, 2021, pp. 465–482.
URL https://www.usenix.org/conference/usenixsecurity21/presentation/khandelwal

[77] P. G. Kelley, L. F. Cranor, N. Sadeh, Privacy as part of the app decision-making process, in: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI '13, Association for Computing Machinery, New York, NY, USA, 2013, p. 3393–3402. doi:10.1145/2470654.2466466.
URL https://doi.org/10.1145/2470654.2466466

[78] V. Mehta, D. Gooch, A. Bandara, B. Price, B. Nuseibeh, Privacy care: A tangible interaction framework for privacy management, ACM Trans. Internet Technol. 21 (1) (Feb. 2021). doi:10.1145/3430506.
URL https://doi.org/10.1145/3430506

[79] O. Drozd, S. Kirrane, Privacy cure: Consent comprehension made easy, in: M. Hölbl, K. Rannenberg, T. Welzer (Eds.), ICT Systems Security and Privacy Protection, Springer International Publishing, Cham, 2020, pp. 124–139. doi:10.1007/978-3-030-58201-2_9.
URL https://doi.org/10.1007/978-3-030-58201-2_9

[80] F. R. P. Couto, S. D. Zorzo, Privacy negotiation mechanism in internet of things environments, in: Americas Conference on Information Systems 2018: Digital Disruption, AMCIS 2018, AISEL, New Orleans, Lousiana, USA, 2018.

[81] R. Tucker, C. Tucker, J. Zheng, Privacy pal: Improving permission safety awareness of third party applications in online social networks,

in: 2015 IEEE 17th international conference on high performance computing and communications, 2015 IEEE 7th international symposium on cyberspace safety and security, and 2015 IEEE 12th international conference on embedded software and systems, IEEE, New York, NY, USA, 2015, pp. 1268–1273. doi:10.1109/HPCC-CSS-ICESS.2015.83.
URL https://doi.org/10.1109/HPCC-CSS-ICESS.2015.83

[82] A. C. Squicciarini, M. Shehab, J. Wede, Privacy policies for shared content in social network sites, The VLDB Journal 19 (6) (2010) 777–796. doi:10.1007/s00778-010-0193-7.
URL https://doi.org/10.1007/s00778-010-0193-7

[83] A. C. Squicciarini, D. Lin, S. Sundareswaran, J. Wede, Privacy policy inference of user-uploaded images on content sharing sites, IEEE transactions on knowledge and data engineering 27 (1) (2014) 193–206. doi:10.1109/TKDE.2014.2320729.
URL https://doi.org/10.1109/TKDE.2014.2320729

[84] H. Lee, A. Kobsa, Privacy preference modeling and prediction in a simulated campuswide iot environment, in: 2017 IEEE International Conference on Pervasive Computing and Communications (PerCom), IEEE, New York, NY, USA, 2017, pp. 276–285. doi:10.1109/PERCOM.2017.7917874.
URL https://doi.org/10.1109/PERCOM.2017.7917874

[85] A. Ratikan, M. Shikida, Privacy protection based privacy conflict detection and solution in online social networks, in: International conference on human aspects of information security, privacy, and trust, Springer, Cham, 2014, pp. 433–445. doi:10.1007/978-3-319-07620-1_38.
URL https://doi.org/10.1007/978-3-319-07620-1_38

[86] S. Barth, D. Ionita, M. D. De Jong, P. H. Hartel, M. Junger, Privacy rating: A user-centered approach for visualizing data handling practices of online services, IEEE transactions on professional communication 64 (4) (2021) 354–373. doi:10.1109/TPC.2021.3110617.
URL https://doi.org/10.1109/TPC.2021.3110617

[87] D. A. Albertini, B. Carminati, E. Ferrari, Privacy settings recommender for online social network, in: 2016 IEEE 2nd International Conference on Collaboration and Internet Computing (CIC), IEEE,

New York, NY, USA, 2016, pp. 514–521. doi:10.1109/CIC.2016.079.
URL https://doi.org/10.1109/CIC.2016.079

[88] M. Ataei, A. Degbelo, C. Kray, Privacy theory in practice: designing a user interface for managing location privacy on mobile devices, Journal of Location Based Services 12 (3-4) (2018) 141–178. doi:10.1080/17489725.2018.1511839.
URL https://doi.org/10.1080/17489725.2018.1511839

[89] B. C. Singh, B. Carminati, E. Ferrari, Privacy-aware personal data storage (p-pds): Learning how to protect user privacy from external applications, IEEE Transactions on Dependable and Secure Computing 18 (2) (2019) 889–903. doi:10.1109/TDSC.2019.2903802.
URL https://doi.org/10.1109/TDSC.2019.2903802

[90] T. Kandappu, V. Subbaraju, Q. Xu, Privacyprimer: Towards privacy-preserving episodic memory support for older adults, Proc. ACM Hum.-Comput. Interact. 5 (CSCW2) (Oct. 2021). doi:10.1145/3476047.
URL https://doi.org/10.1145/3476047

[91] S. Prange, A. Shams, R. Piening, Y. Abdelrahman, F. Alt, Priview–exploring visualisations to support users' privacy awareness, in: Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, CHI '21, Association for Computing Machinery, New York, NY, USA, 2021. doi:10.1145/3411764.3445067.
URL https://doi.org/10.1145/3411764.3445067

[92] S.-H. Kim, I.-Y. Ko, S.-H. Kim, Quality of private information (qopi) model for effective representation and prediction of privacy controls in mobile computing, Computers & Security 66 (2017) 1–19. doi:10.1016/j.cose.2017.01.002.
URL https://doi.org/10.1016/j.cose.2017.01.002

[93] O. de Paula Albuquerque, M. Fantinato, P. C. Hung, S. M. Peres, F. Iqbal, U. Rehman, M. U. Shah, Recommendations for a smart toy parental control tool, The Journal of Supercomputing 78 (8) (2022) 11156–11194.
URL https://doi.org/10.1007/s11227-022-04319-4

[94] D. Lin, D. Steiert, J. Morris, A. Squicciarini, J. Fan, Remind: Risk estimation mechanism for images in network distribution, IEEE Transactions on Information Forensics and Security 15 (2020) 539–552. doi:10.1109/TIFS.2019.2924853.
URL https://doi.org/10.1109/TIFS.2019.2924853

[95] J. M. Such, N. Criado, Resolving multi-party privacy conflicts in social media, IEEE Transactions on Knowledge and Data Engineering 28 (7) (2016) 1851–1863. doi:10.1109/TKDE.2016.2539165.
URL https://doi.org/10.1109/TKDE.2016.2539165

[96] E. Aghasian, S. Garg, L. Gao, S. Yu, J. Montgomery, Scoring users' privacy disclosure across multiple online social networks, IEEE Access 5 (2017) 13118–13130. doi:10.1109/ACCESS.2017.2720187.
URL https://doi.org/10.1109/ACCESS.2017.2720187

[97] Y. Guo, F. Liu, T. Zhou, Z. Cai, N. Xiao, Seeing is believing: Towards interactive visual exploration of data privacy in federated learning, Information Processing & Management 60 (2) (2023) 103162.
URL https://doi.org/10.1016/j.ipm.2022.103162

[98] O. R. Sanchez, I. Torre, B. P. Knijnenburg, Semantic-based privacy settings negotiation and management, Future Generation Computer Systems 111 (2020) 879–898.
URL https://doi.org/10.1016/j.future.2019.10.024

[99] K. Olejnik, I. Dacosta, J. S. Machado, K. Huguenin, M. E. Khan, J.-P. Hubaux, Smarper: Context-aware and automatic runtime-permissions for mobile devices, in: 2017 IEEE Symposium on Security and Privacy (SP), IEEE, New York, NY, USA, 2017, pp. 1058–1076. doi:10.1109/SP.2017.25.
URL https://doi.org/10.1109/SP.2017.25

[100] H. Kaur, I. Echizen, R. Kumar, Smart data agent for preserving location privacy, in: 2020 IEEE Symposium Series on Computational Intelligence (SSCI), IEEE, New York, NY, USA, 2020, pp. 2567–2575. doi:10.1109/SSCI47803.2020.9308396.
URL https://doi.org/10.1109/SSCI47803.2020.9308396

[101] A. de Lima Salgado, F. S. Dias, J. a. P. R. Mattos, R. P. de Mattos Fortes, P. C. K. Hung, Smart toys and children's privacy: usable privacy policy insights from a card sorting experiment, in: Proceedings of the 37th ACM International Conference on the Design of Communication, SIGDOC '19, Association for Computing Machinery, New York, NY, USA, 2019. doi:10.1145/3328020.3353951.
URL https://doi.org/10.1145/3328020.3353951

[102] G. Bal, K. Rannenberg, J. I. Hong, Styx: Privacy risk communication for the android smartphone platform based on apps' data-access behavior patterns, Computers & Security 53 (2015) 187–202. doi:10.1016/j.cose.2015.04.004.
URL https://doi.org/10.1016/j.cose.2015.04.004

[103] M. Kay, M. Terry, Textured agreements: re-envisioning electronic consent, in: Proceedings of the Sixth Symposium on Usable Privacy and Security, SOUPS '10, Association for Computing Machinery, New York, NY, USA, 2010. doi:10.1145/1837110.1837127.
URL https://doi.org/10.1145/1837110.1837127

[104] P. Wijesekera, A. Baokar, L. Tsai, J. Reardon, S. Egelman, D. Wagner, K. Beznosov, The feasibility of dynamically granted permissions: Aligning mobile privacy with user preferences, in: 2017 IEEE Symposium on Security and Privacy (SP), IEEE, New York, NY, USA, 2017, pp. 1077–1093. doi:10.1109/SP.2017.51.
URL https://doi.org/10.1109/SP.2017.51

[105] M. Gisch, A. De Luca, M. Blanchebarbe, The privacy badge: a privacy-awareness user interface for small devices, in: Proceedings of the 4th International Conference on Mobile Technology, Applications, and Systems and the 1st International Symposium on Computer Human Interaction in Mobile Technology, Mobility '07, Association for Computing Machinery, New York, NY, USA, 2007, p. 583–586. doi:10.1145/1378063.1378159.
URL https://doi.org/10.1145/1378063.1378159

[106] A. Alabduljabbar, A. Abusnaina, U. Meteriz-Yildiran, D. Mohaisen, Tldr: Deep learning-based automated privacy policy annotation with key policy highlights, in: Proceedings of the 20th Workshop on Workshop on Privacy in the Electronic Society, WPES '21, Association

for Computing Machinery, New York, NY, USA, 2021, p. 103–118. doi:10.1145/3463676.3485608.
URL https://doi.org/10.1145/3463676.3485608

[107] P. Shayegh, S. Ghanavati, Toward an approach to privacy notices in iot, in: 2017 IEEE 25th International Requirements Engineering Conference Workshops (REW), IEEE, New York, NY, USA, 2017, pp. 104–110. doi:10.1109/REW.2017.77.
URL https://doi.org/10.1109/REW.2017.77

[108] T. Orekondy, B. Schiele, M. Fritz, Towards a visual privacy advisor: Understanding and predicting privacy risks in images, in: 2017 IEEE International Conference on Computer Vision, IEEE, New York, NY, USA, 2017, pp. 3706–3715. doi:10.1109/ICCV.2017.398.
URL https://doi.org/10.1109/ICCV.2017.398

[109] N. Vishwamitra, Y. Li, H. Hu, K. Caine, L. Cheng, Z. Zhao, G.-J. Ahn, Towards automated content-based photo privacy control in user-centered social networks, in: Proceedings of the Twelfth ACM Conference on Data and Application Security and Privacy, CODASPY '22, Association for Computing Machinery, New York, NY, USA, 2022, p. 65–76. doi:10.1145/3508398.3511517.
URL https://doi.org/10.1145/3508398.3511517

[110] G. Akkuzu, B. Aziz, M. Adda, Towards consensus-based group decision making for co-owned data sharing in online social networks, IEEE Access 8 (2020) 91311–91325. doi:10.1109/ACCESS.2020.2994408.
URL https://doi.org/10.1109/ACCESS.2020.2994408

[111] L.-E. Holtz, K. Nocun, M. Hansen, Towards displaying privacy information with icons, in: S. Fischer-Hübner, P. Duquenoy, M. Hansen, R. Leenes, G. Zhang (Eds.), Privacy and Identity Management for Life, Springer Berlin Heidelberg, Berlin, Heidelberg, 2011, pp. 338–348.
URL https://doi.org/10.1007/978-3-642-20769-3_27

[112] N. Vishwamitra, Y. Li, K. Wang, H. Hu, K. Caine, G.-J. Ahn, Towards pii-based multiparty access control for photo sharing in online social networks, in: Proceedings of the 22nd ACM on Symposium on Access Control Models and Technologies, Association for Computing Machinery, New York, NY, USA, 2017, p. 155–166. doi:

10.1145/3078861.3078875.
URL https://doi.org/10.1145/3078861.3078875

[113] J. Angulo, S. Fischer-Hübner, T. Pulls, E. Wästlund, Towards usable privacy policy display & management, in: HAISA, Centre for Security, Communications & Network Research - University of Plymouth, London, UK, 2011, pp. 108–118.

[114] T. Munemasa, M. Iwaihara, Trend analysis and recommendation of users' privacy settings on social networking services, in: International Conference on Social Informatics, Springer, Cham, 2011, pp. 184–197. doi:10.1007/978-3-642-24704-0_23.
URL https://doi.org/10.1007/978-3-642-24704-0_23

[115] A. Aktypi, J. R. Nurse, M. Goldsmith, Unwinding ariadne's identity thread: Privacy risks with fitness trackers and online social networks, in: Proceedings of the 2017 on Multimedia Privacy and Security, MPS '17, Association for Computing Machinery, New York, NY, USA, 2017, p. 1–11. doi:10.1145/3137616.3137617.
URL https://doi.org/10.1145/3137616.3137617

[116] C. Villaràn, M. Beltràn, User-centric privacy for identity federations based on a recommendation system, Electronics 11 (8) (2022) 1238.
URL https://doi.org/10.3390/electronics11081238

[117] P. G. Kelley, P. Hankes Drielsma, N. Sadeh, L. F. Cranor, User-controllable learning of security and privacy policies, in: Proceedings of the 1st ACM Workshop on Workshop on AISec, AISec '08, Association for Computing Machinery, New York, NY, USA, 2008, p. 11–18. doi:10.1145/1456377.1456380.
URL https://doi.org/10.1145/1456377.1456380

[118] K. Alemerien, User-friendly privacy-preserving photo sharing on online social networks, Journal of Mobile Multimedia 16 (2020) 267–292.
URL https://doi.org/10.13052/jmm1550-4646.1631

[119] Y. Wang, L. Gou, A. Xu, M. X. Zhou, H. Yang, H. Badenes, Veilme: An interactive visualization tool for privacy configuration of using personality traits, in: Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, CHI '15, Association

for Computing Machinery, New York, NY, USA, 2015, p. 817–826. doi:10.1145/2702123.2702293.
URL https://doi.org/10.1145/2702123.2702293

[120] A. Aydin, D. Piorkowski, O. Tripp, P. Ferrara, M. Pistoia, Visual configuration of mobile privacy policies, in: International Conference on Fundamental Approaches to Software Engineering, Springer Link, Uppsala, Sweden, 2017, pp. 338–355. doi:10.1007/978-3-662-54494-5_19.
URL https://doi.org/10.1007/978-3-662-54494-5_19

[121] D. Reinhardt, J. Borchard, J. Hurtienne, Visual interactive privacy policy: The better choice?, in: Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, CHI '21, Association for Computing Machinery, New York, NY, USA, 2021. doi:10.1145/3411764.3445465.
URL https://doi.org/10.1145/3411764.3445465

[122] F. Karegar, T. Pulls, S. Fischer-Hübner, Visualizing exports of personal data by exercising the right of data portability in the data track - are people ready for this?, in: IFIP International Summer School on Privacy and Identity Management, Springer International Publishing, Cham, 2016, pp. 164–181. doi:10.1007/978-3-319-55783-0_12.
URL https://doi.org/10.1007/978-3-319-55783-0_12

[123] J. Kolter, M. Netter, G. Pernul, Visualizing past personal data disclosures, in: 2010 International Conference on Availability, Reliability and Security, IEEE, New York, NY, USA, 2010, pp. 131–139. doi:10.1109/ARES.2010.51.
URL https://doi.org/10.1109/ARES.2010.51

[124] J. Kang, H. Kim, Y. G. Cheong, J. H. Huh, Visualizing privacy risks of mobile applications through a privacy meter, in: International Conference on Information Security Practice and Experience, Springer International Publishing, Cham, 2015, pp. 548–558. doi:10.1007/978-3-319-17533-1_37.
URL https://doi.org/10.1007/978-3-319-17533-1_37

[125] M. Netter, M. Weber, M. Diener, G. Pernul, Visualizing social roles - design and evaluation of a bird's-eye view of social network privacy

settings, in: M. Avital, J. M. Leimeister, U. Schultze (Eds.), 22st European Conference on Information Systems, ECIS 2014, Tel Aviv, Israel, June 9-11, 2014, Association for Information Systems, Tel Aviv, Israel, 2014. doi:10.5283/epub.29793.
URL https://doi.org/10.5283/epub.29793

[126] W. Brunotte, L. Chazette, L. Kohler, J. Klunder, K. Schneider, What about my privacy?helping users understand online privacy policies, in: Proceedings of the International Conference on Software and System Processes and International Conference on Global Software Engineering, ICSSP '22, Association for Computing Machinery, New York, NY, USA, 2022, p. 56–65. doi:10.1145/3529320.3529327.
URL https://doi.org/10.1145/3529320.3529327

[127] R. Liu, J. Cao, K. Zhang, W. Gao, J. Liang, L. Yang, When privacy meets usability: Unobtrusive privacy permission recommendation system for mobile apps based on crowdsourcing, IEEE Transactions on Services Computing 11 (5) (2018) 864–878. doi:10.1109/TSC.2016.2605089.
URL https://doi.org/10.1109/TSC.2016.2605089

[128] L. Fang, L. Yin, Q. Zhang, F. Li, B. Fang, Who is visible: Resolving access policy conflicts in online social networks, in: GLOBECOM 2017 - 2017 IEEE Global Communications Conference, IEEE, New York, NY, USA, 2017, pp. 1–6. doi:10.1109/GLOCOM.2017.8254015.
URL https://doi.org/10.1109/GLOCOM.2017.8254015