Privacy Nutrition Labels: Promise, Practice, and Paradoxes in Communicating Privacy *

Bishnu Bhusal[1], Yuanye Ma[2], and Rohit Chadha[1]

[1] University of Missouri, Columbia MO 65211, USA
{bhusalb, chadhar}@missouri.edu
[2] Discovery Partners Institute, University of Illinois, Chicago IL 60606, USA
yuanyem@uillinois.edu

Abstract. Privacy nutrition labels have emerged as a compelling alternative to lengthy, complex privacy policies for effectively communicating privacy information. In recent years, research on privacy nutrition labels has expanded significantly. However, a literature review of privacy nutrition labels is still lacking. To address this gap, we created and analyzed a dataset of privacy nutrition label papers from 2009 to 2024. We qualitatively coded the papers published in the past 15 years, and revealed characteristics of existing privacy labels research. Our findings highlight areas that have received more attention and those that remain underserved. Our analysis also shed light on common methodologies in existing studies and the different communities of stakeholders. We conclude by reflecting on the gaps in existing research and discussing where future work can focus on.

Keywords: Privacy labels · Literature survey · Qualitative analysis.

1 Introduction

Privacy policies have traditionally been the primary way organizations communicate data practices, but their complexity and evolving digital landscapes have led to alternative methods. These include web-based cookie consent notices [29], privacy icons [31], and tailored mechanisms for new interfaces, such as robots [73], often combining text with voice, shapes, and visuals. Privacy labels or privacy nutrition labels were first proposed by [55] as a concise alternative to lengthy policies, and have gained traction after Apple and Google mandated them in 2020 and 2022 [46]. Despite their potential, privacy labels introduced challenges, including inaccuracies, inconsistencies with privacy policies, etc [4,40,50].

Privacy labels, designed to serve diverse communities and purposes, present significant opportunities for HCI research and interdisciplinary collaboration. To map this field and identify areas for impactful collaboration, we present a review paper summarizing existing research on privacy communication, focusing on privacy labels. As the field grows, our survey examines its current state, historical

* Rohit Chadha and Bishnu Bhusal were partially supported by NSF CCF 1900924.

context, research gaps, norms, and provides an entry point for newcomers. Unlike prior focused reviews, our work offers a broader perspective, emphasizing the multidisciplinary nature of privacy label research. We reviewed privacy label research across seven major academic databases: ACM Digital Library, Web of Science, Scopus, IEEE Xplore, ScienceDirect, SpringerLink, arXiv, and Google Scholar. Our research addresses key questions: Who is the focus of privacy label research? What are the goals? What are the most common methods? Are user perspectives considered? What gaps exist in current research? This paper characterizes the field, highlights areas of focus and negligence, offers recommendations for future studies, and provides an open-source dataset of privacy label papers with qualitative codes to support future meta-analyses.

Related work

Existing survey work highlights the multidisciplinary nature of privacy labels, recognizing their complexity and the need to understand them from seven perspectives: business, legal, regulatory, usability and human factors, educative, technological, and multidisciplinary [37,11]. Survey studies have also examined how to design effective privacy communication. One review assessed whether privacy labels fulfill GDPR transparency requirements [60], while others focus on user-centric design. For instance, [5] identified key attributes of privacy visualizations valued by users and experts, and [17] extracted lessons from existing iconography to inform privacy icon design. More recent surveys have explored privacy labels in IoT applications. [65] critiqued IoT privacy labels for primarily targeting owners while neglecting other affected users, advocating for design space exploration. [63] reviewed tools aiding engineers in developing privacy-sensitive IoT applications. [2] proposed a privacy and security label for IoToys, identifying key risk factors and a methodology for evaluating toy privacy and security.

2 Data collection, method, and analysis

Dataset Creation. To identify privacy labels papers from 2009-2024, we queried 7 popular academic databases using the key word "privacy label". Further manual checks were performed on the initial datasets, removing false positives, dissertations, and papers that were considered out of scope for our purpose. Our initial search retrieved 894 papers and, after manual checks, the final datasets consist of 78 papers. In general, privacy label-related research papers have been increasing over the past few years and have exploded since 2021 (see Figure 1).

Analysis. We qualitatively coded the papers using an iterative process by developing and applying a codebook. The initial codebook included deductive codes based on our research questions, such as *communities of focus*, *methods*, etc. The three authors then went through two rounds of independently applying and updating the codebook, using a randomly selected set of 30 papers for each

iteration. After each round, the authors came together to compute interrater reliability (IRR) using Krippendorff's alpha [47], refine or eliminate codes, add new codes. The final codebook included 7 overarching codes with 2-9 subcodes each. The final codebook is summarized in Table 1. Full code definitions can be found in the Supplementary Materials [8].

3 Key Findings

We report the findings using the coding schema, which has seven major categories that collectively provide a rich description of the field of research on privacy communication from different angles and perspectives.

Category	Mean IRR	Multiple	Code	Papers/Code	Code Only
Comm	0.39 (SD=0.14)	✓	Developer	23 (29.5%)	18 (23.1%)
			User	52 (66.7%)	42 (53.8%)
			Regulator	10 (12.8%)	5 (6.4%)
			HCI Designer	5 (6.4%)	1 (1.3%)
Timing	0.45 (SD=0.1)	×	Before	46 (59.0%)	46 (59.0%)
			After	11 (14.1%)	11 (14.1%)
			Independent	19 (24.4%)	19 (24.4%)
Method	0.71 (SD=0.1)	✓	Survey App	27 (34.6%)	7 (9.0%)
			Survey User/Dev	23 (29.5%)	6 (7.7%)
			Lit Review	11 (14.1%)	9 (11.5%)
			NLP	12 (15.4%)	3 (3.8%)
			Focus/Interview	20 (25.6%)	5 (6.4%)
			Static	14 (17.9%)	2 (2.6%)
			Dynamic	15 (19.2%)	0 (0.0%)
			Usability	16 (20.5%)	2 (2.6%)
Platform	0.74 (SD=0.28)	✓	Google	25 (32.1%)	12 (15.4%)
			iOS	33 (42.3%)	20 (25.6%)
			IoT	9 (11.5%)	9 (11.5%)
			Other	3 (3.8%)	3 (3.8%)
			Independent	21 (26.9%)	21 (26.9%)
Product	0.54 (SD=0.13)	✓	Tool	24 (30.8%)	21 (26.9%)
			Recommendation	56 (71.8%)	53 (67.9%)
Issues	0.62 (SD=0.21)	✓	AppLabel	7 (9.0%)	3 (3.8%)
			AppPolicy	2 (2.6%)	0 (0.0%)
			PolicyLabel	4 (5.1%)	0 (0.0%)
			Crossplatform	4 (5.1%)	2 (2.6%)
			Labelselect	11 (14.1%)	8 (10.3%)
			Labelupdate	2 (2.6%)	1 (1.3%)
			Effectiveness	23 (29.5%)	17 (21.8%)
			Alternative	26 (33.3%)	20 (25.6%)
			Compliance	14 (17.9%)	5 (6.4%)
Third-party	0.61 (SD=0)	×	Third-party-Y/N	21 (26.9%)	21 (26.9%)

Table 1. The final codebook comprises 7 main code categories and 32 subcodes. Columns are defined as follows: **Mean IRR** indicates the mean inter-rater reliability for each category. **Multiple** indicates that multiple codes can apply to the same paper. **Code** identifies the subcodes within each category. **Papers/Code** shows the number and percentage of papers with code. **Code Only** represents the number and percentage of instances where the code is exclusive to the given category.

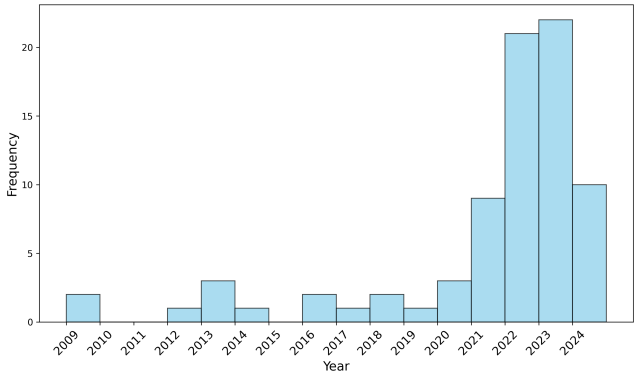

Fig. 1. Distribution of privacy label papers over time (2009-2024).

3.1 Community of focus

The *community of focus* refers to one or multiple specific populations that a study is concerned with. Our analysis has identified four main communities: *developers*, *users*, *HCI designers*, and *regulators*. *Users* are the main focus of most articles, with nearly 80 percent of analyzed papers including *users* as their focus. We applied the *user* code (Comm-user) when articles address issues such as raising awareness of privacy labels, effective communication, or usability concerns. For example, [53] compares the usability of privacy labels of Android and iOS systems. *Developers* are the second most studied community. *Developers* (Comm-developer) refers to mobile app developers. Studies focused on *developers* were concerned with creating tools or recommendations for generating privacy labels. About 57 percent of papers focus on *developers*. For example, [74] explored a tool for developers to create accurate privacy labels. The third community is *HCI designers* (Comm-HCI designer), focusing on innovative privacy communication design. For example, [27] examines the design of icons for understandable privacy information. Finally, *regulators* are the least studied group. *Regulators* (Comm-regulator) refer to government agencies, focusing on compliance with privacy laws like the GDPR. [60] explores whether privacy labels can help data controllers fulfill their transparency obligations under the GDPR.

3.2 Timing

The *timing* code refers to the point of time under which the issue of privacy communication are considered, and hence can be further categorized into three subcode: before acquisition (of an app or device), after acquisition, and independent (where the article does not specify). For example, [7] discusses the effectiveness of Android permissions after the user has acquired the app. [66] offered guidance on creating GDPR-compliant and usable privacy policies regardless of timining. Timing is an implicit factor of privacy labels studies. The papers studied did not necessarily articulate on this. However, this code is important for understanding privacy labels research, because different timining presents various levels of control for users, and may require different design. Our analysis revealed that

most studies focused on privacy communication before acquisition, which may be a result of Google and Apple mandates. As users continue to interact with privacy labels after acquiring the app or device (and after the apps have gone through updates), future work may need to look into after acquisition.

3.3 Method of Study

The *method of study* refers to the one or multiple specific methodologies. Eight primary methodologies have been identified: *surveying apps*, *surveying users or developers*, *literature reviews*, *natural language processing (NLP)*, *focus groups or interviews*, *static code analysis*, *dynamic behavior analysis*, and *usability evaluation*.

3.4 Platform

The code *platform* refers to the environment which a paper focuses on for its study. We have identified five main sub-categories: *iOS*, *Android*, *IoT*, *Other*, and *Independent*. Majority of the papers focus on iOS as the primary environment of study, followed by Android. A growing platform of focus is the Internet of Things (IoT), driven by the increasing popularity of IoT applications. For example, [20] discusses privacy nutrition labels for IoT devices. Papers on platforms like Facebook OS and the web fall under the *Other* category, e.g., [7]. The final category is *Independent*, which includes studies that are not tied to a specific platform. For example, [27] examines the designs of privacy icons.

3.5 Outcome of Study

The *outcome* of a study refers to the final products of the study. For example, [2] offers *recommendations* for creating privacy labels for internet-connected toys to assist parents. [24] develops a *tool* called Privacy Label Wiz to generate privacy labels for iOS apps.

3.6 Issues addressed

Issues addressed refers to the primary challenges and problems that research studies aim to solve or address. We identified nine distinct categories of issues. *AppLabel* focuses on detecting inconsistencies between application behavior and privacy labels, as demonstrated in studies such as [74]. *AppPolicy* examines discrepancies between application behavior and privacy policies, as investigated in works like [52]. *PolicyLabel* analyzes inconsistencies between privacy policies and privacy labels, as explored in research such as [1]. *CrossPlatform* investigates variations in privacy labels across different platforms, as studied in [68]. *LabelSelect* addresses the development and generation of accurate privacy labels, as presented in works like [49]. *LabelUpdate* examines the evolution and modifications of privacy labels over time, as analyzed in studies such as [4]. *Effectiveness* evaluates the impact and utility of privacy labels, as investigated

in research like [32]. *Alternative* explores novel and alternative methodologies for communicating privacy information, as demonstrated in [36]. *Compliance* addresses challenges related to regulatory compliance, including adherence to frameworks such as the GDPR and the California Consumer Privacy Act, as examined in works like [66].

3.7 Third party

The *third party* code refers to whether a paper has examined or discussed third-party libraries. For example, [33] explores inconsistencies between data collection practices of third-party libraries and the privacy labels of Android apps.

4 Discussion and conclusion

Privacy labels research is largely driven by inconsistencies across different privacy communication mechanisms, particularly between privacy labels and policies, as well as discrepancies between platforms like Google and Apple. Privacy labels can only serve as a reliable privacy communication mechanism if these inconsistencies are resolved. Additionally, developers and end-users received the most attention in existing privacy labels research, less has been done from the perspective of regulators. Lastly, third-party libraries pose a significant challenge to creating trustworthy privacy labels, as their data collection and sharing practices often lack transparency, making it difficult to ensure the accuracy and reliability of privacy labels.

Despite the growing body of research on privacy nutrition labels, significant gaps remain. Current studies focus primarily on mobile platforms, particularly iOS and Android, leaving IoT and other emerging technologies underexplored. Future work should prioritize developing standardized methodologies to evaluate the effectiveness of privacy labels across different platforms, address third-party transparency issues, and explore innovative and user-friendly privacy communication strategies beyond labels. By bridging these gaps, research can contribute to more reliable and meaningful privacy communications that improve user trust and regulatory compliance.

References

1. Ali, M.M., Balash, D.G., Kodwani, M., Kanich, C., Aviv, A.J.: Honesty is the best policy: On the accuracy of apple privacy labels compared to apps' privacy policies (2024), `https://arxiv.org/abs/2306.17063`
2. Allana, S., Chawla, S.: Childshield: A rating system for assessing privacy and security of internet of toys. Telematics and Informatics **56**, 101477 (2021)
3. Arkalakis, I., Diamantaris, M., Moustakas, S., Ioannidis, S., Polakis, J., Ilia, P.: Abandon all hope ye who enter here: A dynamic, longitudinal investigation of android's data safety section. In: 33rd USENIX Security Symposium (USENIX Security 24). pp. 5645–5662. USENIX Association, Philadelphia, PA (Aug 2024)

4. Balash, D.G., Ali, M.M., Wu, X., Kanich, C., Aviv, A.J.: Longitudinal analysis of privacy labels in the apple app store (2023), https://arxiv.org/abs/2206.02658
5. Barth, S., Ionita, D., Hartel, P.: Understanding online privacy—a systematic review of privacy visualizations and privacy by design guidelines. ACM Computing Surveys (CSUR) **55**(3), 1–37 (2022)
6. Barth, S., Ionita, D., de Jong, M.D.T., Hartel, P.H., Junger, M.: Privacy rating: A user-centered approach for visualizing data handling practices of online services. IEEE Transactions on Professional Communication **64**(4), 354–373 (Dec 2021)
7. Benton, K., Camp, L.J., Garg, V.: Studying the effectiveness of android application permissions requests. In: 2013 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops). pp. 291–296 (March 2013)
8. Bhusal, B., Ma, Y., Chadha, R.: Supplementary materials for the paper privacy nutrition labels: Promise, practice, and paradoxes in communicating privacy, https://github.com/bhusalb/privacy-label-review-paper
9. Bian, B., Ma, X., Tang, H.: The supply and demand for data privacy: Evidence from mobile apps. Available at SSRN 3987541 (2021)
10. Carter, S.E., d'Aquin, M., Spagnuelo, D., Tiddi, I., Cormican, K., Felzmann, H.: The privacy-value-app relationship and the value-centered privacy assistant. arXiv preprint arXiv:2308.05700 (2023)
11. Caven, P.J., Gopavaram, S., Dev, J., Camp, L.J.: Sok: Anatomy of effective cybersecurity label development. Available at SSRN 4591786 (2023)
12. Chen, C., Shu, D., Ravishankar, H., Zeng, Y., Jain, L., Agarwal, Y., Cranor, L.F.: Ask the consumers: What should be on iot privacy & security labels? Poster presented at the Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023) (2023)
13. Chen, C.C., Shu, D., Ravishankar, H., Li, X., Agarwal, Y., Cranor, L.F.: Is a trustmark and qr code enough? the effect of iot security and privacy label information complexity on consumer comprehension and behavior. In: Proceedings of the CHI Conference on Human Factors in Computing Systems. CHI '24, Association for Computing Machinery, New York, NY, USA (2024)
14. Cranor, L.F.: Necessary but not sufficient: Standardized mechanisms for privacy notice and choice. J. on Telecomm. & High Tech. L. **10**, 273 (2012)
15. Cranor, L.F.: Mobile-app privacy nutrition labels missing key ingredients for success. Commun. ACM **65**(11), 26–28 (Oct 2022)
16. Drozd, O., Kirrane, S.: A conceptual consent request framework for mobile devices. Information **14**(9) (2023)
17. Edwards, L., Abel, W.: The use of privacy icons and standard contract terms for generating consumer trust and confidence in digital services. CREATe Working Paper Series (2014)
18. Emami-Naeini, P., Agarwal, Y., Cranor, L.F.: Specification for CMU IoT security and privacy label. Tech. rep., Carnegie Mellon University (jan 2021), https://iotsecurityprivacy.org/downloads/Privacy_and_Security_Specifications.pdf
19. Emami-Naeini, P., Agarwal, Y., Faith Cranor, L., Hibshi, H.: Ask the experts: What should be on an iot privacy and security label? In: 2020 IEEE Symposium on Security and Privacy (SP). pp. 447–464 (May 2020)
20. Emami-Naeini, P., Dheenadhayalan, J., Agarwal, Y., Cranor, L.F.: An informative security and privacy 'nutrition' label for internet of things devices. IEEE Security and Privacy **20**(2), 31 – 39 (2022)

21. Fox, G., Lynn, T., Rosati, P.: Enhancing consumer perceptions of privacy and trust: a gdpr label perspective. Information Technology & People **35**(8), 181–204 (2022)
22. Fox, G., Tonge, C., Lynn, T., Mooney, J.G.: Communicating compliance: Developing a gdpr privacy label. In: Americas Conference on Information Systems (2018)
23. Gardner, J., Feng, Y., Jain, A., Sadeh, N.: Privacy label wiz: Helping ios application developers create accurate privacy labels. Poster presented at the Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022) (2022)
24. Gardner, J., Feng, Y., Reiman, K., Lin, Z., Jain, A., Sadeh, N.: Helping mobile application developers create accurate privacy labels. In: 2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). pp. 212–230 (June 2022)
25. Garg, R., Telang, R.: Impact of app privacy label disclosure on demand: An empirical analysis. Available at SSRN 4588747 (2022)
26. Goncalves Pontes, D.R., Zorzo, S.D., Moreira de Mello, J.S.: 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 (2017), 23rd Americas Conference on Information Systems (AMCIS), Boston, MA, 2017
27. von Grafenstein, M., Kiefaber, I., Heumüller, J., Rupp, V., Graßl, P., Kolless, O., Puzst, Z.: Privacy icons as a component of effective transparency and controls under the gdpr: effective data protection by design based on art. 25 gdpr. Computer Law & Security Review **52**, 105924 (2024)
28. Guo, W., Rodolitz, J., Birrell, E.: Poli-see: An interactive tool for visualizing privacy policies. In: Proceedings of the 19th Workshop on Privacy in the Electronic Society. p. 57–71. WPES'20, Association for Computing Machinery, New York, NY, USA (2020)
29. Habib, H., Li, M., Young, E., Cranor, L.: "okay, whatever": An evaluation of cookie consent interfaces. In: Proceedings of the 2022 CHI conference on human factors in computing systems. pp. 1–27 (2022)
30. Heid, K., Andrae, V., Heider, J.: Towards detecting device fingerprinting on ios with api function hooking. In: Proceedings of the 2023 European Interdisciplinary Cybersecurity Conference. pp. 78–84. Association for Computing Machinery (2023)
31. Holtz, L.E., Nocun, K., Hansen, M.: Towards displaying privacy information with icons. In: Privacy and Identity Management for Life: 6th IFIP WG 9.2, 9.6/11.7, 11.4, 11.6/PrimeLife International Summer School, Helsingborg, Sweden, August 2-6, 2010, Revised Selected Papers 6. pp. 338–348. Springer (2011)
32. Hutton, H.J., Ellis, D.A.: Exploring user motivations behind ios app tracking transparency decisions. In: Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems. CHI '23, Association for Computing Machinery, New York, NY, USA (2023)
33. Inayoshi, H., Kakei, S., Saito, S.: Detection of inconsistencies between guidance pages and actual data collection of third-party sdks in android apps. In: Proceedings of the IEEE/ACM 11th International Conference on Mobile Software Engineering and Systems. pp. 43–53 (2024)
34. Jain, A., Rodriguez, D., Del Alamo, J.M., Sadeh, N.: Atlas: Automatically detecting discrepancies between privacy policies and privacy labels. In: 2023 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). pp. 94–107. IEEE (2023)

35. Jain, V., Ghanavati, S., Peddinti, S.T., McMillan, C.: Towards fine-grained localization of privacy behaviors. In: 2023 IEEE 8th European Symposium on Security and Privacy (EuroS&P). pp. 258–277 (July 2023)
36. Jesus, V., Pandit, H.J.: Consent receipts for a usable and auditable web of personal data. IEEE Access **10**, 28545–28563 (2022)
37. Johansen, J., Pedersen, T., Fischer-Hübner, S., Johansen, C., Schneider, G., Roosendaal, A., Zwingelberg, H., Sivesind, A.J., Noll, J.: A multidisciplinary definition of privacy labels. Information & Computer Security **30**(3), 452–469 (2022)
38. Kelley, P.G.: Designing a privacy label: assisting consumer understanding of online privacy practices. In: CHI '09 Extended Abstracts on Human Factors in Computing Systems. p. 3347–3352. CHI EA '09, Association for Computing Machinery, New York, NY, USA (2009)
39. Kelley, P.G., Bresee, J., Cranor, L.F., Reeder, R.W.: 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)
40. Khandelwal, R., Nayak, A., Chung, P., Fawaz, K.: Comparing privacy labels of applications in android and ios. In: Proceedings of the 22nd Workshop on Privacy in the Electronic Society. p. 61 – 73. Association for Computing Machinery, Inc (2023)
41. Khandelwal, R., Nayak, A., Chung, P., Fawaz, K.: The overview of privacy labels and their compatibility with privacy policies. arXiv preprint arXiv:2303.08213 (2023)
42. Khandelwal, R., Nayak, A., Chung, P., Fawaz, K., Bianchi, A., Celik, Z.B., Yarom, Y., Shen, X.S., Fang, Z., Zhang, S., et al.: Unpacking privacy labels: A measurement and developer perspective on google's data safety section. In: 33rd USENIX Security Symposium (USENIX Security 24). pp. 2831–2848 (2024)
43. Koch, S., Altpeter, B., Johns, M.: The ok is not enough: A large scale study of consent dialogs in smartphone applications. In: 32nd USENIX Security Symposium, USENIX Security 2023. vol. 8, p. 5467 – 5484. USENIX Association (2023)
44. Koch, S., Wessels, M., Altpeter, B., Olvermann, M., Johns, M.: Keeping privacy labels honest. Proceedings on Privacy Enhancing Technologies (2022)
45. Kollnig, K., Shuba, A., Van Kleek, M., Binns, R., Shadbolt, N.: Goodbye tracking? impact of ios app tracking transparency and privacy labels. In: Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency. p. 508–520. FAccT '22, Association for Computing Machinery, New York, NY, USA (2022)
46. Krämer, J.: The death of privacy policies: How app stores shape gdpr compliance of apps. Krämer, J.(2024). The death of privacy policies: How app stores shape GDPR compliance of apps. Internet Policy Review **13**(2) (2024)
47. Krippendorff, K.: Content analysis: An introduction to its methodology. Sage publications (2018)
48. Krupp, B., Hadden, J., Matthews, M.: An analysis of web tracking domains in mobile applications. In: Proceedings of the 13th ACM Web Science Conference 2021. p. 291–298. WebSci '21, Association for Computing Machinery, New York, NY, USA (2021)
49. Li, T., Cranor, L.F., Agarwal, Y., Hong, J.I.: Matcha: An ide plugin for creating accurate privacy nutrition labels. Proc. ACM Interact. Mob. Wearable Ubiquitous Technol. **8**(1) (mar 2024)
50. Li, T., Reiman, K., Agarwal, Y., Cranor, L.F., Hong, J.I.: Understanding challenges for developers to create accurate privacy nutrition labels. In: Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems. CHI '22, Association for Computing Machinery, New York, NY, USA (2022)

51. Li, Y., Chen, D., Li, T., Agarwal, Y., Cranor, L.F., Hong, J.I.: Understanding ios privacy nutrition labels: An exploratory large-scale analysis of app store data. In: Extended Abstracts of the 2022 CHI Conference on Human Factors in Computing Systems. CHI EA '22, Association for Computing Machinery, New York, NY, USA (2022)
52. Lie, D., Austin, L.M., Sun, P.Y.P., Qiu, W.: Automating accountability? privacy policies, data transparency, and the third party problem. University of Toronto Law Journal **72**(2), 155 – 188 (2021)
53. Lin, Y., Juneja, J., Birrell, E., Cranor, L.F.: Data safety vs. app privacy: Comparing the usability of android and ios privacy labels. Proceedings on Privacy Enhancing Technologies (2024)
54. Liu, D., Xiao, Y., Zhang, C., Xie, K., Bai, X., Zhang, S., Xing, L.: iHunter: Hunting privacy violations at scale in the software supply chain on iOS. In: 33rd USENIX Security Symposium (USENIX Security 24). pp. 5663–5680. USENIX Association, Philadelphia, PA (Aug 2024)
55. McDonald, A.M., Cranor, L.F.: The cost of reading privacy policies. Isjlp **4**, 543 (2008)
56. McDonald, A.M., Lowenthal, T.: Nano-notice: Privacy disclosure at a mobile scale. Journal of Information Policy **3**, 331–354 (2013)
57. McParlan, J., van der Linden, D.: Privacy labels should go to the dogs. In: Proceedings of the Eight International Conference on Animal-Computer Interaction. ACI '21, Association for Computing Machinery, New York, NY, USA (2022)
58. Morel, V., Pardo, R.: Sok: Three facets of privacy policies. In: Proceedings of the 19th Workshop on Privacy in the Electronic Society. p. 41–56. WPES'20, Association for Computing Machinery, New York, NY, USA (2020)
59. Nguyen, T.T., Backes, M., Stock, B.: Freely given consent? studying consent notice of third-party tracking and its violations of gdpr in android apps. In: Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security. p. 2369–2383. CCS '22, Association for Computing Machinery, New York, NY, USA (2022)
60. Novović, M.: Privacy nutrition labels, app store and the gdpr: Unintended consequences? Journal of Data Protection & Privacy **5**(3), 267–280 (2022)
61. Pan, S., Hoang, T., Zhang, D., Xing, Z., Xu, X., Lu, Q., Staples, M.: Toward the cure of privacy policy reading phobia: Automated generation of privacy nutrition labels from privacy policies (2023)
62. Pan, S., Tao, Z., Hoang, T., Zhang, D., Xing, Z., Xu, X., Staples, M., Lo, D.: Seeprivacy: Automated contextual privacy policy generation for mobile applications (2023)
63. Perera, C., Barhamgi, M., Vecchio, M.: Envisioning tool support for designing privacy-aware internet of thing applications. IEEE Internet of Things Magazine **4**(1), 78–83 (2021)
64. Gonçalves de Pontes, D.R., Zorzo, S.D.: Ppmark: An architecture to generate privacy labels using tf-idf techniques and the rabin karp algorithm. In: Latifi, S. (ed.) Information Technology: New Generations. pp. 1029–1040. Springer International Publishing, Cham (2016)
65. Prange, S., Alt, F.: Increasing users' privacy awareness in the internet of things: Design space and sample scenarios. In: Human Factors in Privacy Research, pp. 321–336. Springer International Publishing Cham (2023)
66. Renaud, K., Shepherd, L.A.: How to make privacy policies both gdpr-compliant and usable. In: 2018 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA). pp. 1–8 (June 2018)

67. Rodriguez, D., Del Alamo, J.M., Fernández-Aller, C., Sadeh, N.: Sharing is not always caring: Delving into personal data transfer compliance in android apps. IEEE Access **12**, 5256–5269 (2024)
68. Rodriguez, D., Jain, A., Alamo, J.M.D., Sadeh, N.: Comparing privacy label disclosures of apps published in both the app store and google play stores. In: 2023 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). pp. 150–157 (July 2023)
69. S. Bargh, M., van de Mosselaar, M., Rutten, P., Choenni, S.: On using privacy labels for visualizing the privacy practice of smes: Challenges and research directions. In: DG.O 2022: The 23rd Annual International Conference on Digital Government Research. p. 166–175. dg.o 2022, Association for Computing Machinery, New York, NY, USA (2022)
70. Scoccia, G.L., Autili, M., Stilo, G., Inverardi, P.: An empirical study of privacy labels on the apple ios mobile app store. In: 2022 IEEE/ACM 9th International Conference on Mobile Software Engineering and Systems (MobileSoft). pp. 114–124 (May 2022)
71. Shen, Y., Vervier, P.A.: Iot security and privacy labels. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) **11498 LNCS**, 136 – 147 (2019)
72. Srinath, M., Narayanan Venkit, P., Badillo, M., Schaub, F., Giles, C., Wilson, S.: Automated detection and analysis of data practices using a real-world corpus. In: Ku, L.W., Martins, A., Srikumar, V. (eds.) Findings of the Association for Computational Linguistics: ACL 2024. pp. 4567–4574. Association for Computational Linguistics, Bangkok, Thailand (Aug 2024)
73. Vitale, J., Tonkin, M., Herse, S., Ojha, S., Clark, J., Williams, M.A., Wang, X., Judge, W.: Be more transparent and users will like you: A robot privacy and user experience design experiment. In: Proceedings of the 2018 ACM/IEEE international conference on human-robot interaction. pp. 379–387 (2018)
74. Xiao, Y., Li, Z., Qin, Y., Bai, X., Guan, J., Liao, X., Xing, L.: Lalaine: Measuring and characterizing Non-Compliance of apple privacy labels. In: 32nd USENIX Security Symposium (USENIX Security 23). pp. 1091–1108. USENIX Association, Anaheim, CA (Aug 2023)
75. Zhang, S., Lei, H., Wang, Y., Li, D., Guo, Y., Chen, X.: How android apps break the data minimization principle: An empirical study. In: 2023 38th IEEE/ACM International Conference on Automated Software Engineering (ASE). pp. 1238–1250 (2023)
76. Zhang, S., Feng, Y., Yao, Y., Cranor, L.F., Sadeh, N.: How usable are ios app privacy labels? Proceedings on Privacy Enhancing Technologies (2022)
77. Zhang, S., Sadeh, N.: Do privacy labels answer users' privacy questions? In: Workshop on Usable Security and Privacy (2023)
78. Zorzo, S.D., De Pontes, D.R.G., Dias, D.H., De Mello, J.S.M.: Privacy rules: Approach in the label or textual format. In: AMCIS 2016: Surfing the IT Innovation Wave - 22nd Americas Conference on Information Systems. Association for Information Systems (2016)