Supporting Materials

Table 1 Topics, Research Methods, and Research Areas

Topic researched	**Method used**	**Reference to paper**	**Research area**
Users' privacy concerns and their privacy preferences, personality differences, and behavioural reactions. Value of privacy	between-subject **online experiment Survey**	(Pu & Grossklags, 2015)	Applications (Social App)- App adoption
Privacy concerns of the user, their privacy preferences, personality differences, and behavioural reactions and privacy values	a **scenario**-based factorial online **survey**	(Barbosa et al., 2019; Pu & Grossklags, 2015)	Smart home
Permission Management and Specifying or Inferring Purposes.	Large-scale survey	(Smullen et al., 2020)	Mobile Application
Smart-home devices and related services. Technical vulnerabilities. Configuration challenges. User privacy preferences and incidental users' needs	Focus group and Large-scale **survey**	(Cobb et al., 2021)	Smart home
Quality of privacy practices, and actual behaviour. Analysing policies from financial institutions.	**Mixed methods approach** (automatic quantitative analysis with more qualitative aspects when required.)- just analysis no survey or interview /focus group are involved.	(Shipp & Blasco, 2020)	Finance
Situational factors inform user preferences on online tracking	Semi-structured interviews	(Melicher et al., 2015)	Web tracking- web
Technical term and privacy policy	Pilot study followed by large-scale, quantitative user study **Survey**	(Tang et al., 2021)	Website (shopping behaviour)- Economy
Evaluating Browser Fingerprints (users' perception of browser finger printing, applied	Tow user **surveys**	(Pugliese et al., 2020)	

countermeasures,) trackability of users, Formal Concepts (threat of browser fingerprinting on individuals' privacy). Fingerprinting and User Experience. security and five lay persons.			Browser- web application
Smart Home Privacy Risks and Concerns, Bystanders' Privacy Concern and privacy Mechanisms	Six focus groups (scenario-based discussions)	(Yao et al., 2019)	Smart home
Privacy control and awareness solutions, Informed Consent, Awareness and Risk Communication. Data Leaks and Privacy Visualizations. Glanceable Design to Enhance User Engagement	**Interviews**	(Wilkinson et al., 2020)	Smart phones
User Awareness and Privacy Concerns. Android and iOS Privacy Leakages. Privacy Preserving Solutions	**Interview** and task-based study	(Ramokapane et al., 2019)	Smart Phone
Privacy issue, the example of WebRTC identity. WebRTC identity. Web SSO usage and related work. API and data format limitation,	Field **survey**	(Corre et al., 2017)	Web applications
Perceptions of tracking technologies…. Challenging issues of drone. Privacy mechanisms for drones	In-person **interviews** (Scenario-based questions)	(Y. Wang et al., 2016)	Civilian Drones- High tech products
Risk Perception, Risk Communication,	**Survey** study with 942 participants with between subject study	(Gerber et al., 2019)	New technologies, i.e., Online Social Networks

Privacy and IT Security Risk Awareness and Perception,			(OSN), smart home and smart health devices.
Security and privacy, crowdsourcing (Accuracy of Crowdsourcing, Time Efficiency of Crowdsourcing, With Privacy, Context is King)	Between-subjects study involving the use of an Android mobile app (**Experimental** design) using crowdsourcing approach.	(Bello-Ogunu & Shehab, 2016)	Beacon Encounters-Business / Mobile app
Usability, privacy, and app permissions. Crowd sourcing in the context of smartphone apps and privacy. users' expectations and reactions about privacy-related behaviours and permission.	Experiment	(Ismail et al., 2017)	Crowdscourcing / smart phone
(1) context-free privacy scoring, (2) context-aware privacy scoring, and (3) personalized privacy scoring.	Snowball crawling process *in March 2016 for about a month and collected 31,495,500 tweets from 29,293 users*	(Q. Wang et al., 2019)	Social network
Legal Requirements for Consent Dialog. Technical Solutions for Seeking Consent.	**Survey** instrument (functional mock-up, and exit questionnaire)	(Machuletz & Böhme, 2020)	Website
Data recording and storage, privacy concerns and policies, and user awareness and perceptions. (High level of trust in devices' manufacturers, with little verification behaviour)	Survey	(Malkin et al., 2019)	Smart speakers/ Smart homes/ IoT
Online Threats and Privacy Attacks., The Importance of Mental Models., Older Adults' Online Activities and Behaviours., Using the Internet as a Communication Tool.,	**Interviews** (using drawmetrics) and **online survey** in study 2	(Ray et al., 2020)	Digital privacy

Picture-Drawing Sessions., Older Adults' Perceptions of Privacy.			
Privacy and Security Advice. Mental Models. Adoption of Tools	Online **survey** (with demographically stratified sample)	(Story et al., 2021)	Web tools
Anatomy of an IoT App, (Requirements for IoT Privacy Analysis, Challenges of an IoT Privacy Solution.)	Survey	(Babun et al., 2021)	IoT Applications
User Modelling, Browsers, Settings, and Tools, Notification Preferences	**Mixed methods** (qualitative (n= 186) and quantitative **surveys** (n= 888)).	(Smullen et al., 2021)	Web Browser
1)perceptions of different categories of data, (2) familiarity with the legal framework regarding expectations for privacy controls, (3) awareness of data processing, dataflow, safeguards, and threat models	Mental model study based on semi-structured **interviews**	(Tolsdorf et al., 2021)	GDPR and business
Background on Digitalization in Agriculture, Privacy in Digitalized Agriculture, The Influence of Users' Perception on Privacy Preferences	Empirical study (qualitative) **Survey and focus groups**	(Linsner et al., 2021)	Digital privacy- business
Privacy at Risk. Online Self-Disclosure	Survey	(Lee et al., 2021)	Socioeconomic
Taxonomy of Sharing., Situated Privacy and Security.	Semi-structured **interview and focus group**	(Al-Ameen et al., 2021)	Digital Devices (Online accounts)

Personal Motivation Group Motivation Ease of Adoption. Secure Community. Risk	**Survey** and workshops	(Borradaile et al., 2021)	PGP email encryption adoption
Analysis of Mobile App Privacy. Comparison of Free and Paid Apps. Consumer Expectations and Attitudes [Data Collection and Behavioural Advertising, Paying for Privacy]	Survey	(Han et al., 2020)	Applications (paid application)/ Mobile app
Tor and Jon Donym Research on Technology Acceptance	Online **survey** -Quantitative statistical analysis approach	(Harborth et al., 2020; Mhaidli et al., 2020)	Tor/JonDonym (service/technology)
IoT Privacy Concerns Smart Speaker Privacy. Controls. Leveraging Interpersonal Cues for Privacy. Usability and Perceived Privacy	within-subjects lab **Experiment**	(Mhaidli et al., 2020)	IoT/ smart speakers
Smart devices observed in Airbnbs. Guests' smart device preferences (Factors: Device location, and context) Guests' smart device needs Guests' concerns	Survey	(Mare et al., 2020)	Smart Devices
Adoption and Acceptance of PETs VPNs as PETs... Usability as a Factor in PET Adoption. Judgment and Decision Making. The Technology Adoption Model	**Survey** and pre-test **interviews**	(Namara et al., 2020)	Virtual Private Networks (VPNs)/ (technology service)
Pet wearables and privacy concerns.	**Mixed method** – comparative study (including **survey**)	(van der Linden et al., 2020)	Pets

Understanding consumers through review analysis			
Information Sharing on OSNs. Interdependent Privacy & Game Theory.	Parametric utility functions and Survey	(Olteanu et al., 2019)	Games
Privacy Theory Privacy Iconography Privacy Frameworks	**Qualitative analysis** of 366 drawings of privacy- mental model	(Oates et al., 2018)	Technology,
Privacy Analysis of Mobile Apps Children's Applications	Automated analysis on 5855 android apps (dynamic and static analysis)	(Reyes et al., 2018)	Mobile apps / Children's Online Privacy Protection Act (COPPA),
Prevalence and Usage of Permissions. Personal Data Collection and Dissemination	**In-depth static and dynamic analysis of apps**	(Feal et al., 2020)	Childern's parental control, mobile application
Information Privacy Concern [Genesis of IUIPC (The scale Internet Users' Information Privacy Concern (IUIPC)]. The Role of Privacy Concern Scales in the Investigation of PETs. Validity and Reliability [Content Validity, Construct Validity, Reliability]	Survey	(Groß, 2021)	Validity, Reliability information privacy
Privacy Challenges of Video Analytics. Sampling and Modelling Privacy Preferences. Privacy Attitudes-Factors Impacting Privacy Attitudes [Allow/Deny Decisions, Comfort Level, Surprise Level, and Notification Preference]	Experience sampling study	(Zhang et al., 2021)	Video analysis

Correlation Between Privacy Expectations and Allow/Deny Preferences Lack of Awareness and Desire for Greater Transparency			
Transferability, Loss functions to generate adversarial examples for metric networks, Adversarial perturbations to prevent real-world face recognition platforms from correctly tagging a user's face	Between-subject study- User study with 423 participants (**Experimental** design)	(Chandrasekaran et al., 2020)	Adversarial / traceability

Full List for the paper's limitations and gaps/ future work.

1- **For paper 2** (Pu & Grossklags, 2015) , online experiment **Survey**, **limitation on the use of Survey to investigate on the actual behaviour. [**Future work should also con-sider direct behavioural measures of interdependent privacy valuations to account for a potential discrepancy between survey measures and **actual behaviours** [1, 99]**] + [**additional work is needed to further identify and investigate factors that contribute to the concern for friends' privacy in this particular scenario**]**

2- **From paper 4** (Smullen et al., 2020) limitation on the use of **survey** in **measuring possible contextual factors, and another limitation regarding self-reporting and actual configuration of privacy settings [**It is not possible to enumerate and measure the significance of every possible contextual factor that may have had an influence on participants' responses, prior research has shown that both self-reported privacy **preferences and actual configuration** of privacy settings are malleable].

3- **From paper 3** (Barbosa et al., 2019; Pu & Grossklags, 2015)**,** a Scenario-based factorial online survey**, there is a lack on the research around predicting what make individuals accept/deny of information flow, also the subjective comfort levels that the survey can measure [..In** predicting changes to preferences, our approach only predicts the direction of changes and the relative contribution of a situational factor toward such changes. It would be useful to also predict what could make people accept or deny an information flow, in other words, what could change their mind**.].**

4- **Paper 14** (Corre et al., 2017) , **Field survey describing the** implementation limitation of the protocol.

5- **Paper 16** (Gerber et al., 2019) **, Survey** study cultural limitation based on the targeted uses. Recruitment method might also limit the user sample [we used a **panel** to recruit our participants, thus it is likely that our sample is biased in terms of age, academic background and technical expertise, as it might be younger, higher educated and overly tech-savvy] applying **a between-subject design**. [The results are expected to be (at least slightly) different if we had used a within-subject design].

6- **Paper 20** (Machuletz & Böhme, 2020) , **Survey** instrument (functional mock-up, and exit questionnaire), [**experimental** setup may not fully reflect **users' actual behaviour** regarding consent dialogs.] also there is user sample bias. [unknown biases due to participant self-selection, which is an acute problem of empirical privacy research [67, 68]. Precisely the attitudes and beliefs of interest correlate with non-response and dropouts].

7- **Paper 21** (Malkin et al., 2019) **Survey**, same size limit to generalize the results. And the methodology bias of the user sample age …etc.

8- **Paper 26** (Story et al., 2021) **online survey instrument** with a demographically stratified sample, [, since we relied on self-reported behaviour, participants' responses may be biased [50]] []

9- **Paper 27** (Babun et al., 2021) , **Survey**, the evaluation of semantically limited strings related to these two privacy labels requires more sophisticated analysis.

10- **Paper 31** (Lee et al., 2021) **Survey, sample bias, the study focusses on** explicit forms of self-disclosure **which does not capture all instance of self-discloser, this might affect [**discrepancies between individuals' recollection of sharing and **their actual disclosure**]. **Future work** [can investigate potential remedies to offer an equitable environment for all individuals' privacy understanding and control.]

11- **Paper 33** (Borradaile et al., 2021) , **workshop** and **survey** limitation [Response Bias, Demographic Bias. Workshop Variation]

12- **Paper 34** (Han et al., 2020) , Survey, static analysis limited to [permissions explicitly declared by apps, not whether apps attempt to gain access to resources]. And the dynamic analysis [relied heavily on a random input generator].

13- **Paper 35** (Harborth et al., 2020; Mhaidli et al., 2020) , .

14- **Paper 37 Survey** (Mare et al., 2020) , results cannot be generalized.

15- **Paper 38** (Namara et al., 2020) **Survey and pre-test interviews**, self-reported bias (social desirability, and memory bias). [since we conducted a survey rather than an interview, we lacked the opportunity to follow up with respondents regarding answers we found interesting]. Gender bias towards men.

16- **Paper 44 Survey,** (Groß, 2021) , limited generation (self-report instruments including, instructional manipulation checks/attention checks). [a self-selection bias due to Prolific's match making] [**Factor analyses ..** are affected by sampling and measurement errors]

17- **From paper 5** (Cobb et al., 2021) , **focus group** and Large-scale **survey**, **social dynamics in real life might limit the conversations between entities, thus further study is needed for incidental user experience [**Real-world social dynamics and power imbalances (especially between device owner employers and incidental user employees) may limit the effectiveness of these conversations, so these specific situations of incidental user experiences are important to explore further.**]**

18- **Paper 8** (Tang et al., 2021) **Pilot study** followed by large-scale, quantitative user study **survey, fail to detect if users are [**between users with partial knowledge of a term and users with no knowledge of the term**.] for future work researchers [**indicates that more in-depth analysis using qualitative methods can be useful to solve the issue.**]**

19- **Paper 40** (Olteanu et al., 2019) , Parametric utility functions and **survey**, [We quantified only a limited number of preference factors ,.. user (reported) privacy attitudes do not always correspond to **actual behaviours].**

20- **Paper 6** (Shipp & Blasco, 2020) **Mixed method approach, the qualitative analysis limits the scalability of the results [**Part of our methodology includes the execution of qualitative analysis that have to be executed manually. Whilst we used these methods to ensure accuracy in our results, we also acknowledge that this limits the scalability of our analysis if it were to be applied to the whole menstru app ecosystem**]**

21- **Paper 28** (Smullen et al., 2021) **mixed methods (**qualitative (n= 186) and quantitative surveys (n= 888)**), results from the qualitative data cannot be generalized. There is also limitation [**Our qualitative data collection and analysis method has limitations to generalizability. The resulting corpus of quantitative preferences used in our experiments are similarly limited, and our results may not scale linearly to the number of website categories or individual websites a user typically encounters compared to our sample…. whose expressed preferences do not completely coincide with **actual decisions** made by users in-situ.**]**

22- **Paper 39** (van der Linden et al., 2020) **mixed methods (including survey)-** comparative study**,** culture representation limitation, fake reviews in the samples. Used [purposive sampling strategy to extract reviews from Amazon. Because privacy concerns may differ depending on sensors contained in a wearable [45].]

23- **Paper 7** (Melicher et al., 2015) **Interviews, bias in the results [**Our data was collected via *after-the-fact interviewing.* Interviews conducted in this way are not without bias participants may alter their opinions in the interview to rationalize their past behaviour. However, this bias is likely to oppose the bias in previous work, which uses *hypothetical survey methodology* [24, 30, 37**]]**

24- **Paper 12** (Wilkinson et al., 2020) **interviews , results might not show the context provided in an interview settings have an influence on the user actual behaviour in comparison to their real life setting with actual screen lock, etc. as it has been discussed in the literature** ['privacy paradox' [49] which implies that users may find new privacy tools useful in controlled settings, but their reaction and use may be significantly diminished when said tool is used in practice**.] future studies [**may want to consider methodological options that would allow participants to investigate different combinations of granularity to further explore users' preferences.]

25- **Paper 13** (Ramokapane et al., 2019) **interviews** with **task based the sampling has basis [**we adopted **convenience sampling** due to limited resources and geographical proximity,**]**

26- **Paper 25** (Ray et al., 2020) **survey and Interviews** (using drawmetrics), [Using drawmetrics offers considerable promise for eliciting perceptions of complex phenomena such as privacy. However, when used as a sole method of gathering data, it does not always succeed in providing awareness of the depth of issues faced by participants]. Using online survey in Study 2 [Using an **online survey** to evaluate mental models comes with some limitations. For one, there is no opportunity to ask follow-up questions.]

27- **Paper 29** (Tolsdorf et al., 2021) **Mental model study based on semi-structured interviews, generalization problem and bias of participants perception by macro-environmental factors like culture [**capture general mental models of informational self-determination at work, generalization of results cannot be given due to the qualitative property of the study and the strong context dependence of privacy.] [our study also contains limitations which are well known in privacy research: our participants' perceptions are biased by macro-environmental factors] [The results of studies with a mental model approach are limited by the study's setting, tasks, and analysis [27]].

28- **Paper 32** (Al-Ameen et al., 2021) , **semi-structured interview and focus group,** [we do not draw any quantitative, generalizable conclusion from this study**.] Sampling bias from using snowball.** In addition**, self-reported data** might have limitations, li**ke recall and observer bias**[users' security and privacy perceptions are positively influenced by their knowledge and technical efficacy [44, 55, 71].

29- **Paper 15** (Y. Wang et al., 2016) **in person interviews with scenario-based questions which may not cover the topic comprehensively [**, the list of our scenarios is by no means comprehensive. We chose realistic scenarios that are already happening in the real world because they would be easier for people to understand.**]**

30- **Paper 17** (Bello-Ogunu & Shehab, 2016) **between subject study- experimental design, using crowdsourcing approach**, one limitation that users [may often weigh utility over privacy and security when making decisions]. Future work [An extension to this research could include explicitly investigating the role of utility to maintain a more honest level of context.] there are scope limitations **on using the concept of contextual integrity** [When considering the privacy labels for beacons, the study examines primarily the "context of flow of information" aspect of contextual integrity, specifically the per-beacon and per-audience context of a flow of information. [An extension to the study could additionally focus on the other components of contextual integrity, such as type of information involve][Another logical extension is to explore the principles of transmission] **Concerning the user study design**, another limitation was the presence of "Average User Concern" in the user interface for those in the CrowdCat group. [This may have somewhat artificially inflated the findings of the privacy label analysis, and more extensive experiments are required to make truly conclusive results.]

31- **Paper 18** (Ismail et al., 2017) **experiment**, limited number of the apps limits the generalization, user sample age and. privacy biases using crowd scouring.

32- **Paper 46** (Chandrasekaran et al., 2020) **Experiment,** Between-subject study. [similar to all other adversarial example generation strategies, is the ever-improving robustness of black-box models [45]].

33- **Paper 36** (Mhaidli et al., 2020), **Experiment [**not generalizable to all real-world**] [partici**pants' behaviour might have differed from circumstances in daily life, i.e., in real world circumstances people might not have the need for privacy at the forefront of their minds, and so the privacy controls might not be as effective] **future research could [**examine participants' **real world behaviours** through field studies to confirm the extent to which the proposed privacy controls are effective at muting the microphone when it is not needed under different conditions**]**

34- **Paper 30** (Linsner et al., 2021) , **Empirical study** (**Survey and focus groups**) since the study was qualitative, no quantitative insights can be gained from it.

35- **Paper 11** (Yao et al., 2019), **focus groups** with **scenario-based discussions, includes co-design activities (exploratory approach)** [scenarios in the study were by no means exhaustive in terms of different application contexts] Future work [can either investigate a more diverse set of scenarios or come up with different contextual factors so that participants can assemble their scenarios]. [our focus group and the co-design activity only included a bystanders' perspective. The co-design activity, although insightful, was also limited by the duration of the study.] Future research ... [, we did not critically evaluate

bystanders' designs in terms of their usability, feasibility, and potential consequences.] Future research.

Others

36- Paper 41 (Oates et al., 2018), Qualitative analysis of 366 drawings of privacy- mental model, [conclusions are limited by our use of secondary data, the use of drawings, and the inherent difficulties of qualitative visual analysis]. [There are also challenges inherent in using drawing as a research tool. Drawing skill level varied among our illustrators.] [Some illustrators may have leaned on cultural rather than personal conceptions of privacy in their drawings].

37- Paper 42 (Reyes et al., 2018) , Automated analysis on 5855 android apps (dynamic and static analysis), [We note that the Monkey does not exhaustively execute all code paths in apps. While it does find a number of potential privacy violations, many more may exist].

38- Paper 43 (Feal et al., 2020), in depth static and dynamic analysis of apps [Despite combining static and dynamic analysis, we acknowledge that our analysis cannot guarantee full coverage of the code, app features, or the data flows][we perform our dynamic analysis on the children app, and it may be that the companion parent app disseminates sensitive data over the network].

39- Paper 45 (Zhang et al., 2021), Experience sampling study, results are not representative of the general population. [data provided by participants when presented with plausible deployment scenarios, rather than based on observations in the presence of actual deployments] [limitation on the phrasing of these types of **scenarios** ...it might have primed participants in one direction or the other].

40- Paper 19 (Q. Wang et al., 2019), Snowballing crawling process (two), [statistical learning approach, false positives/negatives are practically unavoidable, especially due to the subjective nature of privacy perception] Future work [the effective integration of privacy scoring and classification will be beneficial, especially for personalized privacy protection. Privacy scoring with consideration of the audience, and the integration of privacy scoring with access control, are both challenging research questions].

Table 2 Research Areas and Research Methods

Research areas	Research Methods	Paper Reference
Smart Technologies	Survey, interviews, focus group and experiments	(Barbosa et al., 2019; Pu & Grossklags, 2015) (Cobb et al., 2021) (Yao et al., 2019) (Malkin et al., 2019) (Gerber et al., 2019) (Wilkinson et al., 2020) (Ramokapane et al., 2019)

		(Mhaidli et al., 2020) (Ismail et al., 2017) (Mare et al., 2020)
Web applications	Mixed methods (qualitative and quantitative surveys), interviews and Surveys	(Melicher et al., 2015) (Smullen et al., 2021) (Tang et al., 2021) (Machuletz & Böhme, 2020) (Pugliese et al., 2020) (Corre et al., 2017) (Story et al., 2021)
Mobile Applications and pets' wearables	Survey, experiment, and apps (dynamic and static) analysis	(Smullen et al., 2020) (Bello-Ogunu & Shehab, 2016) (Han et al., 2020) (Reyes et al., 2018) (Feal et al., 2020)
Specific demographic groups and pets	In-depth and Automated static and dynamic analysis of apps, survey combined with other methods.	(Reyes et al., 2018) (Feal et al., 2020) (van der Linden et al., 2020)

Smart Technology

Topic researched	**Method used**	**Reference to paper**
Privacy concerns of the user, their privacy preferences, personality differences, and behavioural reactions and privacy values	a **scenario**-based factorial online **survey**	(Barbosa et al., 2019; Pu & Grossklags, 2015)

Smart-home devices and related services. Technical vulnerabilities. Configuration challenges. User privacy preferences and incidental users' needs	Focus group and Large-scale **survey**	(Cobb et al., 2021)
Smart Home Privacy Risks and Concerns, Bystanders' Privacy Concern and privacy Mechanisms	Six **focus groups** (scenario-based discussions)	(Yao et al., 2019)
Data recording and storage, privacy concerns and policies, and user awareness and perceptions. (High level of trust in devices' manufacturers, with little verification behaviour)	Survey	(Malkin et al., 2019)
Risk Perception, Risk Communication, Privacy and IT Security Risk Awareness and Perception,	**Survey** study with 942 participants with between subject study	(Gerber et al., 2019)
Privacy control and awareness solutions, Informed Consent, Awareness and Risk Communication. Data Leaks and Privacy Visualizations. Glanceable Design to Enhance User Engagement	**Interviews**	(Wilkinson et al., 2020)
User Awareness and Privacy Concerns. Android and iOS Privacy Leakages. Privacy Preserving Solutions	**Interview** and task-based study	(Ramokapane et al., 2019)
IoT Privacy Concerns Smart Speaker Privacy. Controls. Leveraging Interpersonal Cues for Privacy. Usability and Perceived Privacy	within-subjects lab **Experiment**	(Mhaidli et al., 2020)

Usability, privacy, and app permissions. Crowd sourcing in the context of smartphone apps and privacy. users' expectations and reactions about privacy-related behaviours and permission.	Experiment	(Ismail et al., 2017)
Smart devices observed in Airbnbs. Guests' smart device preferences (Factors: Device location, and context) Guests' smart device needs Guests' concerns	Survey	(Mare et al., 2020)

Web applications

Topic researched	Method used	Reference to paper
Situational factors inform user preferences on online tracking	Semi-structured **interviews**	(Melicher et al., 2015)
User Modelling, Browsers, Settings, and Tools, Notification Preferences	**Mixed methods** (qualitative (n= 186) and quantitative **surveys** (n= 888)).	(Smullen et al., 2021)
Technical term and privacy policy	Pilot study followed by large-scale, quantitative user study **Survey**	(Tang et al., 2021)
Legal Requirements for Consent Dialog. Technical Solutions for Seeking Consent.	**Survey** instrument (functional mock-up, and exit questionnaire)	(Machuletz & Böhme, 2020)
Evaluating Browser Fingerprints (users' perception of browser finger printing, applied countermeasures,) trackability of users, Formal Concepts (threat of browser fingerprinting on individuals' privacy). Fingerprinting and User Experience. security and five lay persons.	Tow user **surveys**	(Pugliese et al., 2020)
Privacy issue, the example of WebRTC identity. WebRTC identity. Web SSO usage and related work. API and data format limitation,	Field **survey**	(Corre et al., 2017)
Privacy and Security Advice. Mental Models. Adoption of Tools	Online **survey** (with demographically stratified sample)	(Story et al., 2021)

Mobile Applications

Topic researched	Method used	Reference to paper
Permission Management and Specifying or Inferring Purposes.	Large-scale **survey**	(Smullen et al., 2020)
Security and privacy, crowdsourcing (Accuracy of Crowdsourcing, Time Efficiency of Crowdsourcing, With Privacy, Context is King)	Between-subjects study involving the use of an Android mobile app (**Experimental** design) using crowdsourcing approach.	(Bello-Ogunu & Shehab, 2016)
Analysis of Mobile App Privacy. Comparison of Free and Paid Apps. Consumer Expectations and Attitudes [Data Collection and Behavioural Advertising, Paying for Privacy]	Survey	(Han et al., 2020)
Privacy Analysis of Mobile Apps Children's Applications	Automated analysis on 5855 android apps (dynamic and static analysis)	(Reyes et al., 2018)
Prevalence and Usage of Permissions. Personal Data Collection and Dissemination	**In-depth study** of the Android parental control app's ecosystem. study 46 apps from 43 developers which have a combined 20M installs in the Google Play Store	(Feal et al., 2020)

Specific demographic groups and pets

Topic researched	Method used	Reference to paper
Privacy Analysis of Mobile Apps Children's Applications	Automated analysis on 5855 **android apps** (dynamic and static analysis)	(Reyes et al., 2018)
Prevalence and Usage of Permissions. Personal Data Collection and Dissemination	**In-depth static and dynamic analysis of apps**	(Feal et al., 2020)
Pet wearables and privacy concerns. Understanding consumers through review analysis	**Mixed method** – comparative study (including **survey**)	(van der Linden et al., 2020)