A Systematic Survey of Empirical User Studies of Unintentional Information Disclosure in Everyday Digital Interaction

Reza Shahriari
University of Florida
Gainesville, Florida, USA
rshahriari@ufl.edu

Eric D. Ragan
University of Florida
Gainesville, Florida, USA
eragan@ufl.edu

ABSTRACT

The exchange of personal information in digital environments poses significant risks, including identity theft, privacy breaches, and data misuse. Addressing these challenges requires a deep understanding of user behavior and mental models in diverse contexts. This paper presents a systematic literature review of empirical user studies on unintentional information disclosure in usable security, covering 101 papers published across six leading conferences from 2018 to 2023. The studies are categorized based on methodologies—quantitative and qualitative—and analyzed for their applications in various scenarios. Major subtopics, including data privacy, security in browsers, and privacy tools, are examined to highlight research trends and focal areas. This review provides details on topics and application areas that have received the most research attention. Moreover, by comparing descriptive and experimental approaches, findings aim to guide researchers of strategies to mitigate risks associated with online everyday interaction.

KEYWORDS

Usable Security, Human-Computer Interaction

1 INTRODUCTION

Online browsing and app usage are integral to both our personal and professional lives as people depend on various tools and applications to navigate the digital world. Engaging in activities such as exchanging, submitting, and sharing information through emails [65, 118], social media [6, 69], or other digital platforms [22, 127] is commonplace. However, the online exchange of information comes with significant challenges and risks, particularly concerning privacy and security. There is always a potential for unauthorized access and data breaches, which can lead to the release of personal and sensitive information, resulting in identity theft, financial loss, and other malicious activities.

To address online privacy and security issues, people adopt various protective behaviors [14, 128]. These include downloading apps only from reliable and trusted sources and ensuring that the software they use meets high security and privacy standards. Additionally, they may seek to stay informed about potential threats by keeping up with security incidents affecting their families, friends, or the broader community, which helps them identify and avoid similar risks [66, 128]. Furthermore, they adjust their privacy settings to control who can access their information and posts, and they exercise caution before sharing personal details that malicious parties could misuse [14, 21].

Despite these efforts, only a limited number of users consistently familiarize themselves with or follow these risk prevention measures. Therefore, it is crucial to develop software and tools with well-established default security standards to minimize risks. Understanding how people engage with the digital world is essential for identifying specific challenges. The field of usable security and privacy (USP) helps identify these challenges at the intersection of human behavior and digital security [91]. USP helps security experts focus on critical risk areas, enabling more analysis of people's behavioral patterns and ultimately enhancing overall online safety.

While USP is a broad research area, this review specifically concentrates on the subtopic of online information disclosure in everyday digital interactions. We use the term information disclosure to describe situations in which users, often unintentionally, reveal personal or sensitive data through routine online activities such as web browsing, email, or social media use. This focus reflects a consistent pattern in prior empirical studies, which examine how users make decisions about sharing, withholding, or managing data in digital environments. Studying this area is critical because users' privacy and security are shaped not only by technical safeguards but also by individual choices about data sharing and software settings.

Additionally, people may struggle to grasp the nuances of potential information disclosure through different problems, vulnerabilities, and risks. The dependencies on various applications and types of data further complicate this understanding. Because of the need to understand user choice, human-subjects research methodology is commonly employed to study user behaviors and thinking. Different choices of user studies, such as controlled experiments using hypothetical cases or surveys that reflect more realistic personal experiences, provide varying degrees of control and insight. Experiments may offer more control but often rely on hypothetical scenarios, whereas surveys, though less controlled, may capture more authentic personal experiences. Differences in user study types directly affect the knowledge gained, making it crucial to consider the overlap among methods applied, research subtopics focused on, and types of applications studied.

This review aims to highlight the value of a systematic literature review in organizing and assessing the research methods applied across different areas of information disclosure. This will assist future researchers in selecting practical approaches for their studies and ultimately help lower users' online risks. It provides an

YYYY(X), 1–17

https://doi.org/XXXXXXX.XXXXXXX

overview of areas that have received more attention and identifies key topics that could benefit from future work by providing evidence of what research methods have been most effective in different areas. The review spans six leading research conferences in security and human-computer interaction in recent years (2018–2023), filtering from a total of 8185 papers to 101 papers given detailed analysis. We focus on empirical studies involving people, emphasizing the various methods used to conduct user studies. Each method offers unique benefits and limitations. Users have diverse experiences and perspectives that influence their disclosure decisions, which might vary significantly between laboratory settings and real-world contexts. Personal past experiences differ from hypothetical scenarios, and there are distinct challenges in understanding risk when dealing with hypothetical cases versus real personal information.

2 BACKGROUND

2.1 Overview of Usable Security and Privacy

USP aims to make security and privacy mechanisms both accessible and effective by balancing robust protection with user-friendly design. This necessitates a review of key areas where information is at higher risk of disclosure due to the nature of information exchanged or shared. One common topic within USP is *authentication*, which focuses on securing users' online accounts and data by verifying their identities [10, 57, 111]. For instance, when a user logs into an email account, the authentication process ensures that the user is who they claim to be, typically through passwords or other verification methods. In this context, a significant contribution to USP was the development and evaluation of a data-driven password meter, which measures the strength of passwords and provides users with actionable feedback to enhance password security [111].

Another crucial subarea in USP is the study of *user behavior* for security and privacy. This refers to the actions or decisions that individuals take that affect their privacy or data security. For instance, Wu et al. [125] explored how the explanations provided by browsers about private browsing modes shape users' misconceptions and beliefs. Many users incorrectly assumed that private browsing would prevent geolocation tracking, protect against malware, eliminate advertisements, and stop tracking by websites and network providers.

Moreover, differences between expert and non-expert users of the Tor Anonymity Network emphasize the importance of understanding how Tor works to mitigate risks [29]. Experts have a technical understanding of Tor, while non-experts generally see it as a service without detailed knowledge of its operation. This distinction is crucial for reducing the risks of deanonymization and ensuring user safety [29].

Further investigation into why users follow or ignore computer security advice revealed key perception gaps drive these decisions. For example, Fagan et al. [23] found individuals who follow security advice tend to perceive greater benefits and risks in doing so, while those who ignore the advice see higher benefits in not following it. This study highlights the crucial role of users' perceptions in their decision-making regarding computer security [23].

Research in USP also examines users' choices of *security settings*, which are configurable options that help manage or enhance software features for the security and privacy of users and data. These settings include security warnings and indicators that should be easily accessible and understandable for users [3, 13, 25]. Bravo-Lillo et al. [13] explored the design of security-decision user interfaces, introducing attractors to draw attention to critical information in security dialogs, significantly reducing unsafe user actions. On the other hand, Felt et al. [25] focused on browser security indicators, identifying deficiencies in existing designs through surveys of over 1,300 users. They proposed a set of new indicators: Secure for HTTPS, Not secure for HTTP, and Not secure for invalid HTTPS, based on extensive user testing and design considerations.

Another subarea addresses the use of *encryption*, the security method that involves converting information into a coded format to prevent unauthorized access. For instance, Abu-Salma et al. [1] conducted a study to explore obstacles to adopting secure communication tools. Their findings showed that fragmented user bases, incompatible tools, and users' lack of understanding of end-to-end encryption hinder its adoption. Additionally, Whitten and Tygar [121] conducted a usability evaluation of PGP 5.0 [30], a program designed for secure email communication through encryption and digital signatures. Their work [121] highlighted the need for security-specific user interface design principles. They also found that PGP 5.0 is not user-friendly for individuals unfamiliar with cryptography, leading to ineffective use of the security features.

Moreover, the topic of *social engineering* focuses on manipulation techniques that trick individuals into revealing confidential information or providing system access to malicious actors. As an example of work on this topic, Jagatic et al. [45] demonstrated that attackers can easily and effectively exploit social network data to increase the success rate of phishing attacks. It was found that users are over four times more likely to fall victim if solicited by someone appearing to be a known acquaintance [45]. Also, another study [117] explored the effectiveness of different phishing training approaches and found that the impact of the training significantly depends on who delivers it. Facts-and-advice training was more effective when provided by security experts, while stories about phishing incidents were more impactful when shared by peers, showing the importance of the perceived origin of training materials [117].

Our review specifically concentrates on the USP subtopic of online information disclosure in digital interaction, which recognizes the need to protect most individuals who engage in online activities, as these users are often at risk of unintentionally disclosing information. This focus encompasses a range of activities that threaten online users. For instance, users often need to pay more attention to crucial security warnings, thereby missing out on vital information intended to protect them [115]. Privacy concerns are also associated with using online proctoring software during virtual examinations, as these tools often require access to sensitive personal data [107]. Furthermore, sharing personal information on social media platforms can expose individuals to various threats [39], as can the misuse of private browsing features, with users frequently overestimating the level of privacy these functions afford [35]. Additionally, using fitness devices that track and share users' health and location data can pose significant privacy risks if not

properly managed and understood. Each of these areas represents a critical aspect of online user behavior that necessitates careful consideration and study to enhance the safety and privacy of users in the digital world.

A contemporary USP-relevant example is the emerging ecosystem of Digital Identity Wallets being rolled out under the revised eIDAS 2.0 framework in the European Union. The EU Digital Identity Wallet is intended to let citizens store and present verified identity attributes such as ID documents, driving licences, and educational credentials across public and private services through a single mobile wallet [96]. From a usable security and privacy perspective, these wallets introduce new opportunities for unintentional disclosure, as users must navigate fine-grained consent flows, decide which attributes to share in unfamiliar contexts, and reason about how repeated wallet use may link their activities across services. Early empirical work on Digital Identity Wallet concepts shows that users often prioritize convenience and usability over security and privacy, struggle to understand the underlying ecosystem, and request safety nets in case something goes wrong [68, 93]. As EU Member States are required to provide at least one certified wallet by the end of 2026 [96] this represents a high-stakes, real-world setting where effective USP design is crucial to prevent unintentional information disclosure.

2.2 Related Literature Reviews

The literature survey we present in this paper adds to the body of knowledge on online information disclosure and usable security and privacy (USP) literature reviewed by others. Online information disclosure is a critical aspect of USP, as it encompasses the risks and behaviors associated with users' interaction and data-sharing practices. Our review aims to highlight the human factors influencing these interactions and how they align with the findings of previous reviews in the field.

Because our review focuses on human-subjects research, the review by Distler et al. [18] is highly relevant. Their review analyzed papers between 2014–2018 that involved human subject studies to study how researchers represent risk to participants, primarily through simulated or naturally occurring risk. Their investigation also looked into the type of risk representation used across different research methods. They found that papers with an experimental objective mainly employed simulated risk, while descriptive studies primarily used naturally occurring risk. Various tools were used to represent risk to participants, including security/privacy-related tasks, prototypes, and scenarios. Our review, however, differs by focusing on online information disclosure and covering a more recent period (2018–2023), allowing us to compare trends in USP methodology over time.

In addition, Iachello and Hong [43] highlight the critical role of HCI in privacy, emphasizing that many issues stem from user interactions with systems. They call for standard privacy-enhancing techniques, effective analysis methods, and a comprehensive "privacy toolbox". Similarly, Jacobs and McDaniel [44] find that non-expert misunderstandings of technology often lead to risky decisions and security breaches, stressing the need for user education. Garfinkel and Lipford [31] trace the evolution of usable security and privacy, emphasizing that poor usability often results in security failures, advocating for integrating usability and security in design.

Beyond domain-specific reviews, several systematic investigations have also examined methodological approaches in usable security research more broadly. Realpe et al. conducted a systematic review of usability principles, evaluation methods, and development processes for secure authentication systems, concluding that existing methods are fragmented and often insufficiently user-centered for evaluating security-critical interactions [83]. More recently, Sauer et al. compared 22 methods for assessing the relationship between user experience and information security, highlighting substantial variability in methodological scope, data collection strategies, and evaluator roles [92]. Including these perspectives helps position our review within a wider landscape of methodological debates and demonstrates that USP research, like other areas of usable security, lacks consistent empirical approaches.

3 METHODOLOGY

3.1 Research questions

Ensuring the security of individuals participating in online activities is crucial to preventing unintentional disclosure of personal information. This includes addressing various online threats that can harm users. In our review, we focus on online information disclosure in digital interactions, acknowledging the necessity to safeguard most individuals who engage in online activities, as they often risk unintentionally revealing information. This area is chosen due to the significant influence of the user's decision-making process on data sharing and risk-taking. Given the diversity in user experiences and perspectives, it is essential to employ human-subject research to capture this complexity and assess whether certain methods are more effective for specific subtopics. This approach will help us understand if existing results indicate more appropriate methods for the research.

In this work, we sought to analyze research methodology used in USP addressing online information disclosure between 2018–2023. We conducted a systematic literature review of research papers published at top USP venues, filtering to a final set of 101 papers for full analysis. Our analysis focuses on these research questions:

- **RQ1**: For research leveraging human-subjects methods, which topics and application areas have received the most research attention in the study of unintentional online information disclosure, and to what extent is this focus justified given their relevance to everyday digital interactions? Are there underexplored areas or overlaps among topics and applications that merit further investigation?
- **RQ2**: What human-subjects research methods are commonly employed to study unintentional online information disclosure across different topics and application areas? What methodological details, such as participant pool, can guide future researchers in designing studies?

3.2 Systematic Review

This section outlines the methodology employed for conducting the literature review in this survey, providing an overview of its structure. Table 1 provides an overview of the process. Our systematic literature review approach involves four key phases: (1)

publication venue selection, (2) search procedure, (3) filtering, and (4) detailed review.

3.2.1 Publication Venue Selection. The process began by identifying the most relevant peer-reviewed publication venues recognized for emphasizing USP papers, with a particular focus on those that highlight online information disclosure and the threats that users face in digital interaction with the online world. Because USP papers are mainly presented in conference formats, we focused on top-tier venues that (i) are high-impact outlets in security, privacy, and HCI, (ii) consistently publish empirical, human–subjects USP work, and (iii) most directly intersect with explicit online information disclosure. Our search strategy focused on conference proceedings because preliminary screening showed that most empirical studies involving human participants in unintentional disclosure are published in conference venues. Major journals in this domain tend to publish fewer user-centered empirical studies or emphasize technical or policy-focused work that falls outside the scope of our research questions. In addition, we acknowledge that our review is based on a sample of highly relevant venues and that other publications, including journals, may still contain relevant studies.

Balancing scope and feasibility, we selected three flagship conferences in the security and privacy domain: *ACM Conference on Computer and Communications Security (ACM CCS)*, *IEEE Symposium on Security and Privacy (IEEE S&P)*, and *USENIX Security Symposium (USENIX Security)*. In addition, we included two privacy/USP–focused venues with high concentrations of human–subjects studies: the *USENIX Symposium on Usable Privacy and Security (SOUPS)*, which is specifically tailored for USP papers and highly relevant to our study, and the *Privacy Enhancing Technologies Symposium (PETS)*. Lastly, because usable security includes human-centered research, we also included the *ACM Conference on Human Factors in Computing Systems (CHI)*, the premier HCI venue that routinely publishes empirical privacy and security work with human participants.

We considered other strong venues (e.g., ESORICS, EuroS&P, NDSS, CSCW), but excluded them after a scoping pass indicated substantially lower yield of human–subjects studies on online information disclosure relative to the screening effort. We note this as a scope tradeoff and return to it in our limitations. While these six venues are not the only outlets for high-quality USP research, they capture the highest–impact USP and HCI communities

3.2.2 Initial Search Procedure. The next stage of the review method applied term search and listing review to reduce the sample to the most relevant papers from the selected venues and time period. In this stage, we employed two distinct approaches to account for differences in digital libraries and available search capabilities. In the first approach, we utilized the keyword search tools from the ACM Digital Library and the IEEE Xplore Digital Library to create our initial collection of possibly applicable USP papers for *ACM CCS*, *IEEE S&P*, and *ACM CHI*.

To select a set of papers covering user studies for online information disclosure, we first performed an initial filtering using keywords to cover a broad range of potentially relevant papers in usable security that we would later review for specific relevance to information disclosure. We used the keywords to select papers with at least one related term to usable security in addition to one related term to digital interaction in the title or abstract: (*usable security* OR *privacy* OR *security*) AND (*web* OR *online* OR *internet* OR *email*).

We chose these terms because prior USP work shows most explicit online disclosure risks arise through web services, browsers, online communication, and email, not device-local or infrastructure-only contexts. We intentionally did not include broad terms like *IoT*, *authentication*, or *LLM* because they would expand beyond our scope and primarily return papers on mechanisms or platforms where disclosure is not the research focus. In addition to searching through available online digital libraries, the search limitations of specific paper listings necessitated the second approach for some venues. Specifically, we manually reviewed each abstract for USENIX Security, SOUPS, and PETS, which lacked advanced search capabilities in the online digital libraries. Studies on social platforms were still captured because many abstracts/titles use *online*/*web*, and our manual venue passes (SOUPS/PETS/USENIX Security) recovered additional social-media–context papers that the keyword search may miss. This allowed us to identify and include potential papers aligned with our research objectives.

3.2.3 Initial Review and Filtering. During our filtering process, we applied a multi-stage review of titles, abstracts, and full texts to eliminate papers that did not align with our research topic. This stepwise filtering is summarized in Table 1.

Stage 1: Title and keyword screen. We first excluded papers whose titles made it clear they were unrelated to human-subjects research or online interactions. For example, papers describing purely technical mechanisms (e.g., "Side-channel Attacks") or system design papers without a user component were discarded. We also excluded non-archival items such as posters, extended abstracts.

Stage 2: Abstract review. For papers that passed the first screen, we examined abstracts to ensure they (i) included empirical data from human participants and (ii) directly addressed disclosure-related behaviors, perceptions, or risks in online contexts. Examples of *included* papers are those studying willingness to share data with mobile apps or expectations of privacy in video conferencing. Examples of *excluded* papers are those focused solely on tool design without user evaluation, or those studying unrelated topics like cryptographic protocol design, authentication mechanisms, or IoT firmware security.

Stage 3: Full-text eligibility. In the final stage, we reviewed the complete texts to confirm that each paper (i) reported empirical human-subjects data (e.g., surveys, interviews, experiments, diary/log studies), (ii) investigated online information disclosure or user decision-making about sharing/withholding data, and (iii) provided sufficient methodological detail to extract study attributes. Papers failing these criteria, or tool-design papers without empirical user insights, were excluded at this step.

Our research focuses on studying the risks associated with digital interactions in online activities. By applying strict criteria, we ensure precision and relevance in our analysis. This method allows us to comprehensively understand users' information leakage during their browsing or interaction experiences without their awareness.

Filtering Process	Publication Venues						
	ACM CCS	IEEE S&P	USENIX Security	SOUPS	CHI	PETS	**Total**
All published papers	1053	760	1294	187	4381	510	8185
Potential papers after keyword searching and title review	15	23	43	69	60	30	240
Potential papers after filtering with abstract review	1	5	29	41	35	30	141
Included papers after final review	0	3	20	26	25	27	101

Table 1: Filtering selected papers in 6 publication venues between 2018-2023.

3.2.4 Detailed Review. The paper selection and filtering process resulted in a final sample of 101 papers for detailed review. To ensure a thorough analysis, the full text of all final papers was reviewed to gather information on the different research methods used, including surveys, experiments, interviews, and focus groups. Relevant notes, categorizations, and assigned attributes were documented in a spreadsheet to facilitate organization and analysis of this information. Labels were created and updated iteratively over the course of the review. If new labels emerged or new criteria were formed along the way, previously reviewed papers were re-reviewed to ensure consistency. For each paper in the sample, we reviewed and recorded essential information such as the publication venue, topics, end-user context, application areas, research methods, related details, research questions, and research findings. One researcher conducted descriptive coding of 101 included papers. This was done to extract the general context of each paper. Then, two researchers iteratively reviewed the descriptive codes together and performed axial coding to select primary themes. Next, both researchers then iteratively compared and discussed the resulting themes with taxonomies and related topics of other literature (with notable examples including [18], [44]). Both researchers worked together to iterate on the themes and categories until reaching a consensus on the final set. Thus, the papers were distributed across different user experience and behavior topics, such as data privacy and information security, communication and privacy protection, browser-based security and privacy, privacy awareness, perceptions, and behaviors, privacy tools, online advertising, and tracking.

4 FINDINGS OF LITERATURE SURVEY

4.1 Research topic areas in online information disclosure

To identify which topics have received more attention, understand which areas pose higher associated risks, and determine which areas require further research, we needed to develop a set of topic areas. We based our choice of categories on a thorough analysis of the literature on online information disclosure and by coding the 101 papers in our sample. Since no existing taxonomy exactly matched our criteria, we developed our own. This new taxonomy is grounded in existing literature, established taxonomies, and the specific intersections with our paper topic areas.

Each paper was categorized based on its contextual focus for the research into online security and information risk. Following the descriptive coding of the papers, two researchers subsequently conducted a thematic review of the descriptive codes and reached a consensus on larger topic groups. The resulting topics were aggregated into six predominant topic categories, as outlined in Table 2. *Data privacy and information security* leads, capturing 30.7% or 31 out of 101 papers of the research focus. Following this, *communication and privacy protection* secures 21.7% or 22 out of 101 papers, while *browser-based security and privacy* represents 17.8% or 18 out of 101 papers. Additionally, *privacy awareness, perceptions, and behaviors* accounts for 12.9% or 13 out of 101 papers, *privacy tools* comprises 9.9% or 10 out of 101 papers, and finally, *online advertising and tracking* makes up 6.9% or 7 out of 101 papers of the research distribution.

4.1.1 Data privacy and information security. The majority of the papers focus on users' mental models concerning the sharing of personal information with various entities. This topic investigates critical issues surrounding personal data, which is now commonly shared and stored online. It examines security risks linked to the posting of personal data on social media and poor data management practices, such as granting devices access to personal information like location data without understanding how it is managed.

For instance, a study found that many wearable activity tracker users significantly underestimate the number of third-party applications accessing their data, with most users having little understanding of these data-sharing processes [133]. In contrast, research on online proctoring by Terpstra et al. [107] revealed that, under certain conditions, students found it acceptable to share data with their teachers, even when teachers were not directly involved in the proctoring process.

A critical question raised by this research is whether personal data that users have previously shared can ever be permanently deleted from the internet, particularly when shared with companies like Google and Facebook that hold vast amounts of user data. Investigations into users' understanding and expectations of online data deletion in social media and nonspecific contexts highlight users' desires for control over their data and the need for enhanced deletion mechanisms and preferences for data expiration [69, 72].

Additionally, studies using responses to data transparency tools have explored users' concerns and perceptions about data collection by Google and Facebook. These studies found that, while users

appreciate the insight and control provided by these tools, they remain concerned about the amount of data being collected and shared [7, 24].

4.1.2 Communication and privacy protection. This significant area focuses on protecting communications using various platforms, such as email, messaging, and social media. It involves preventing potential risks that users may face, like phishing attempts through emails or the risks associated with using voice assistants or microphones in conferencing tools.

In email security, researchers have examined user decision-making and behaviors when confronted with phishing emails and malicious URLs. For example, many studies concentrate on how different features can help users prevent these risks and understand their behaviors [5, 58, 131]. Interestingly, research found that untrained individuals often outperform phishing filters due to their familiarity and expectations regarding incoming emails [118]. These studies highlight the importance of understanding user thought processes and actions.

The popularity of conferencing tools surged after the COVID-19 pandemic, leading to multiple studies on user behaviors and concerns when using these communication tools. A common finding is that privacy is a top priority for users [22]. However, users often have limited control over their choice of conferencing tools, as these are frequently dictated by their company or colleagues. Detailed investigations, such as one study on the usability issues of the mute button in video conferencing applications, found that while users perceive the mute button as a privacy control, various apps continue to access and even transmit background audio data [127]. This discrepancy between user expectations and actual app behavior underscores a significant usability problem that requires attention to improve user trust and privacy.

In the context of messaging, the primary concern for users is ensuring that their messages remain inaccessible to others. This is achieved through end-to-end encryption, as highlighted in various research papers. These studies delve into users' mental models, behaviors, and misconceptions while using end-to-end encrypted platforms [116]. Interestingly, it was found that visualizing encryption through icons and animations negatively impacted users' perception, while simple text was considered much more trustworthy [102].

4.1.3 Browser-based security and privacy. This topic analyzes the potential threats users might encounter while utilizing web browsers, addressing issues such as users neglecting warnings, installing ad blockers, and misconceptions about using private browsing tools like Tor. The goal is to understand users' mental models and behaviors regarding web features and their privacy, aiming to design intuitive features or educate them on the risks associated with these actions to ensure their online safety and privacy.

Browser extensions are a popular feature among web users, and researchers have studied various aspects of them. For instance, one study examined users' general understanding and preferences regarding the data that extensions can access [46]. Other studies have explored practical use cases, such as using browser extensions to prevent online tracking and addressing usability and breakage issues that users might encounter [64, 75]. These studies also explored whether users stopped using these extensions when faced with breakage.

More technically, the Domain Name System (DNS) is a fundamental web feature that allows users to type the name of a website instead of memorizing its numerical IP address. However, using an untrusted DNS can expose users to unauthorized data access or various types of attacks. Several studies have focused on user awareness and concerns related to different encrypted DNS configurations and settings, as well as the use of an improved version called Protective Domain Name System (PDNS) and its adoption among users [76, 90]. The research found that users mainly trust default configurations and do not customize their settings due to potential breakage. They also tend to adopt the settings used by their Internet Service Provider (ISP).

4.1.4 Privacy awareness, perceptions, and behaviors. Understanding users' behaviors, attitudes, and awareness levels regarding online privacy is crucial because it helps design more effective privacy measures and educational campaigns. By comprehending how users perceive and react to privacy risks, developers and policymakers can create tools and guidelines that better align with users' needs and expectations. This area aims to explore these aspects to comprehend users' expectations and perceptions of privacy. Although it shares similarities with other related topics, the primary focus is on the psychological aspect of users.

For instance, a study on the effect of social norms on privacy behaviors revealed that people tend to disclose sensitive data to avoid disagreeing with others [80]. Individuals often imitate others' behaviors, especially when they perceive that others do not care about privacy. Additionally, the literature highlights the importance of trust in privacy recommendations and the significant role of the source of these recommendations in building trust and encouraging the adoption of guidelines. People primarily educate those in their social circles, emphasizing the significance of trust in privacy-related matters [32].

4.1.5 Privacy tools. Privacy tools encompass a range of features and tools designed to safeguard users' privacy online. These tools offer users a secure and private connection to the internet, protecting them from online threats and prying eyes. However, designing and developing these tools alone is not sufficient; it is equally important to understand users' mental models and scenarios when using these tools. This understanding enables the creation of privacy tools that are more effective, user-friendly, and accessible.

One example of privacy tools is Personal Privacy Assistants (PPAs), which help users manage their privacy online. Research indicates that users prefer PPAs that can learn their preferences, offer high user involvement, allow vendor choice, and provide transparency around data disclosure [101]. By incorporating these preferences, designers can develop more effective and user-friendly PPAs.

Additionally, nudging tools represent another type of privacy tool that can enhance users' privacy. These tools use subtle prompts or reminders to encourage users to take actions that will improve their privacy and security [27, 63, 99]. For instance, a commitment nudge may remind users to install updates, back up their data, or enable two-factor authentication [27]. Moreover, nudging tools

have been used to influence the decision-making behaviors of adolescents using social network services (SNS) to avoid privacy and safety threats [63]. Furthermore, nudging interventions have been utilized to promote the adoption of secure mobile payments [99]. By leveraging these tools, users can take proactive steps to protect their privacy and security online.

4.1.6 Online advertising and tracking. While relatively underrepresented in our sample due to the focus on user studies, online advertising significantly impacts privacy and data protection. Users' personal information and online behavior are analyzed to curate personalized ads, raising concerns about privacy and data protection. Users often remain unaware of the extent to which their personal information is being tracked and used for advertising purposes. This indicates a need for further user studies to explore and address these concerns. For instance, a study demonstrated the impact of hyper-personalized ads on users who had expressed negative emotions and were wary of privacy violations [38]. Another research highlighted the necessity for personalized and interactive ad-targeting explanations that address users' specific concerns [56].

Furthermore, the practice of personalized advertising can seriously affect privacy and security, as this information can be used to track and monitor users without their knowledge or consent. Research has shown that users are not adequately protecting their data even when they feel confident about the type of data being collected [28]. This uncertainty about data utilization can lead to significant privacy risks. For example, while "privacy zones" in fitness tracking apps aim to hide sensitive locations, they have proven to be ineffective [71]. This underscores the urgent need for better privacy protections and user education regarding the use and sharing of location data.

Topic	Number of Papers	Percentage
Data Privacy and Information Security	31	30.7%
Communication and Privacy Protection	22	21.7%
Browser-based Security and Privacy	18	17.8%
Privacy Awareness, Perceptions, and Behaviors	13	12.9%
Privacy Tools	10	9.9%
Online Advertising and Tracking	7	6.9%

Table 2: Distribution of 101 papers across six topics related to privacy and security.

4.2 Application Areas

Whereas the previously-discussed research topics addressed different subareas relevant to online information disclosure, our review also considered whether the studies addressed relevance for specific types of software applications. While some studies addressed general techniques or concepts that were agnostic of specific applications, it is important to identify the different base application types that receive direct attention in empirical research. Following our analysis, the resulting categories of *application areas* were determined based on the specific platforms or categories of software where the research is applied. Whereas most research subtopics are broader and not necessarily tied to specific use cases, the application areas are more concrete for types of software. The purpose of identifying both topics and application areas was to understand the practical contexts in which researchers can gain more specific scenarios that demonstrate how research topics translate into practical applications. They allow for cross-sectional analysis of how a topic is explored across different platforms. For instance, if a leading topic is applied to only one application area, it may suggest a strong research community focus and a potential for saturation, or conversely, the need for more innovative solutions in this area.

Starting with the *browser* application area that accounts for 21.7% of papers and encompasses a wide range of activities, including browser extensions [26, 46, 64], cookie consent interfaces [11, 36], user behavior, and concerns around web browsing privacy [85, 97, 100], etc. It is no surprise that every browser-based security and privacy topic paper explores *browser* application areas. However, only a quarter of papers in online advertising and tracking—the second most popular topic using this area—address this critical area.

Social media applications were identified as another core application area with four topics identified in them, with communication and privacy protection being the most popular, accounting for 36% of usage that investigated different types of privacy protection, such as sharing content [6, 39], account verification and trustworthiness [70, 126] to better to understand users' concerns and needs in the social media context.

Within the *mobile* application domain, there are three topics that focused on these types of applications. An excellent illustration of this is using nudging techniques to encourage the adoption of secure mobile payments, as highlighted in [99]. As an example, [122] demonstrates the effectiveness of data exposure visualizations on mobile devices, further showing the use of this application's versatility across different topics.

Another identified category was *email applications*, which were used mostly for studies of communication and privacy protection (see Figure 1). The review found 32% of app areas focus on this topic and aim to provide a secure and safe space for users when communicating over email. Under this area, some researchers have looked into adopting secure email (e.g., [112]), while others have researched phishing email scenarios in this application area (e.g., [5, 88, 118, 131]).

In addition, many papers from the sample did not focus on a specific application area; rather, they explored broader topics that can be applied across various domains. We organized these papers under the *nonspecific* application area because they are not specific to an application. This category represents the most significant proportion of research papers from the sample, accounting for 41.5%, as shown in Table 3, demonstrating that a large amount of studies cover general concepts or techniques and often aim to be application agnostic. For instance, Sundar and Kim [103] considered users' trust in humans vs machines, while Karunakaran et al. [47] studied users' understanding and opinions about data breaches. Vance et al. [115] also researched the effect of security warnings that users tend to ignore, which can be applied in operating systems and browsers to show potentially malicious websites.

As seen in Figure 1, *nonspecific* application area is substantial for four of the six topics, containing almost more than half of the papers. This highlights the importance of exploring broader topics that can be applied across different domains and enables researchers to uncover fundamental concepts that can benefit multiple domains by studying *nonspecific* application areas, leading to later in-depth analysis of needed areas.

During the application areas review process, we only received a few papers labeled as *operating system* [27], *messaging* [102, 116], and *conferencing tools* [22, 127]. As a result, we decided to merge these and label them as *other* for the application area. As per our analysis, a significant portion (25%) of the papers in this application area falls under online advertising and tracking. However, in three of the topics, there was no mention of this area.

Topic	Number of Papers	Percentage
Nonspecific	42	41.5%
Browser	22	21.7%
Social Media	12	11.8%
Mobile	12	11.8%
Email	8	7.9%
Other	5	4.9%

Table 3: Distribution of application areas in 101 papers

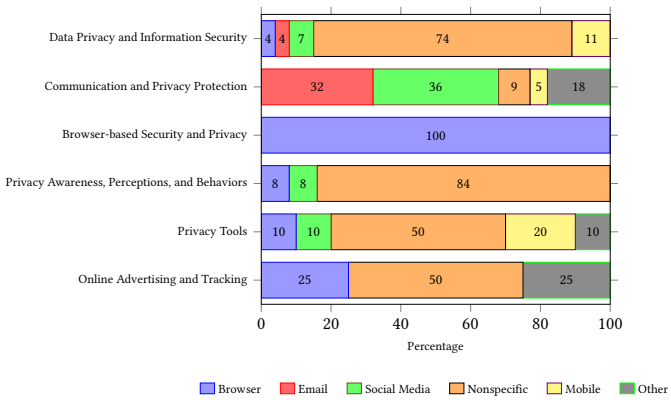

Figure 1: Cross-tab of topics and application areas in percentage

4.3 Research Methods

4.3.1 Overview of Method Types. We categorized types of user research methods following criteria based on Lazar et al. [55]. Our categorization developed by applying the criteria to the findings in the paper sample to result in the following categories of study types: Descriptive and Experimental. The approach for classifying method is similar to Distler et al [18]. However, we omitted the classification of relational studies due to the high dependence on the analysis method over the general method of study and the high frequency of overlap between relational research conducted following descriptive methods. Our analysis found that a majority

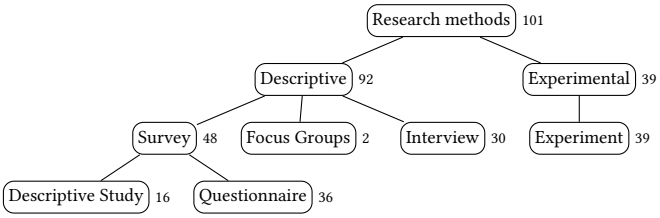

Figure 2: Research methods used in 101 papers

of papers (91.1% or 92 of 101 papers) utilized *descriptive research* methods, as demonstrated in Figure 2. *Descriptive research* aims to describe or identify behaviors or thoughts in a given situation [55]. It often captures data from a natural setting and can serve as a foundation for further study. However, descriptive research only describes what is happening and does not provide insights into the causes behind observed relationships [55]. Types of descriptive research methods found in our review included *surveys*, *focus groups*, and *interviews*. We discuss each of these methods in more detail in the next subsection below.

The review also found a large amount of experimental research, which focuses on comparison or testing hypotheses, often with the goal of testing causal relationships [55]. The review found 38.6% or 39 out of 101 papers utilized experimental research methods. In order to establish cause-and-effect relationships, it is necessary to manipulate conditions and independent variables in a controlled environment and observe outcomes. However, it is important to note that causation and correlation are distinct concepts, and different conditions must be taken into account. Correlation refers to a statistical relationship between two variables, where changes in one variable are associated with changes in another. However, correlation does not imply that one variable causes the change in the other. Causation, on the other hand, indicates that one event is the result of the occurrence of the other event; there is a cause-and-effect relationship. Establishing causation requires more rigorous testing and evidence to show that changes in one variable directly result in changes in another, and that this relationship is not due to other confounding variables. Therefore, simply conducting experiments in a controlled environment does not automatically establish causality. We also discuss this in more detail in the following subsection below. By utilizing both descriptive and experimental research methods, researchers can produce more reliable and accurate results, which can benefit various fields of study.

Research Method	Number of Papers	Percentage
Survey	48	47.5%
Experiment	39	38.6%
Interview	30	29.7%
Analyze Dataset	12	11.8%
Focus Groups	2	1.9%

Table 4: Research methodologies used in 101 papers

4.3.2 Survey. Descriptive studies use surveys as the predominant method to collect information from individuals. Surveys involve

a set of structured questions that are designed to gather specific information from a target population. Surveys are often completed by individuals without the presence of a researcher, which can limit the depth and detail of the data collected. In very small cases, researchers may provide more in-depth insights or explanations and guidance to ensure that questions are properly understood.

The questions can be open-ended or closed-ended. One of the strengths of surveys is their ability to gather a large number of responses from individuals quickly [55]. This allows researchers to capture a wide range of perspectives and opinions on a particular topic.

The surveys were divided into two types: *questionnaires* and *descriptive study*. In our sample, 75% or 36 out of 48 papers that used the survey research method were structured *questionnaires* to collect participant data. These typically involve a set of predetermined questions that are administered to all participants, allowing for standardized data collection and analysis. For example, [17] employed a questionnaire to gather data from 852 participants about the changes in their security and privacy (S&P) behaviors, possible causes for these behaviors, and how they shared these behaviors with others. The results revealed that social triggers, which involve interactions or observations of others, were the most common factor influencing S&P behaviors, with a significant number of participants attributing changes in their behavior to interactions or advice from peers.

This example demonstrates how surveys can be used to collect data from a broad range of participants for age and gender diversity, which was crucial for this study. Surveys using questionnaires also allow data collection without the need for researchers to be present, which can help reduce unintentional researcher bias.

The remaining 25% or 16 out of 48 surveys were classified as descriptive studies. Descriptive studies are a subcategory of survey studies and fall under the umbrella of descriptive research methods that are used to observe and record the characteristics of a phenomenon. In these types of studies, participants engage in specific activities to observe and understand their behaviors and responses. These studies are different than questionnaires that simply ask a set of questions to gather data. For instance, Zimmeck et al. [132] conducted a study where participants were asked to go through a simulated browser setup process and make choices regarding various browser features, including the Global Privacy Control (GPC). The GPC has the potential to empower users to opt out of web tracking efficiently. The participants did not just answer questions—they also actively engaged with a simulated interface to make setup choices that let researchers analyze usability.

4.3.3 Experiment. Experiments offer a controlled environment to explore cause-and-effect relationships, as explained earlier. The main objective of an experiment is to test hypotheses and determine which should be accepted or rejected based on statistical analysis [55]. For example, a study investigated the effectiveness of various measures in helping users identify phishing emails by involving 409 participants who were divided into two groups: one with a tutorial and one without [88]. The goal was to determine the effect of a tutorial on their ability to identify phishing emails. Researchers also exposed each group to different reminder measures, finding that measures based on videos and interactive examples performed best, with their effectiveness lasting for at least another six months.

By dividing the participants into different groups and exposing them to various measures, the researchers could identify which strategies were most effective. This controlled environment allowed for a thorough exploration of cause-and-effect relationships, and statistical analysis was employed to determine which hypotheses should be accepted or rejected.

4.3.4 Interview. Interviews provide valuable data that is difficult to obtain through surveys [55]. They allow researchers to explore thoroughly a problem and gather detailed responses through open-ended questions. Interviews encourage reflection and can reveal valuable insights that may not be captured in surveys.

The use of interviews in research is invaluable for gaining insights into complex issues. For instance, a study interviewed 25 social media users to explore the relationship between the Fear of Missing Out (FoMO) and users' tendencies to compromise their privacy online [106]. Through open-ended questions, the researchers gathered detailed responses about posting habits, joining and staying on platforms, leaving platforms, and perceptions of others' online habits and expectations. Another study used interviews to understand participants' experiences with shared accounts, interviewing 11 online and 14 in-person participants using a semi-structured approach that allowed them to express their thoughts freely [78]. Participants were presented with a categorized list of accounts and asked about their reasons for sharing, challenges when they stopped sharing, and their overall experience. These studies demonstrate the power of interviews in gaining a deeper understanding of complex issues and uncovering insights that may not be captured through other means of data collection.

4.3.5 Focus Groups. Performing interviews is an effective means of data collection, but it can be time-intensive. This is because it necessitates individual meetings with each participant, which may extend to an hour or more per person. An alternative strategy is to utilize focus groups, where multiple participants can engage in collaborative discussions of their opinions, letting researchers gain a deeper understanding [55].

As an example, Zhao et al. [130] conducted research on the online privacy awareness of children who are under 11 years old. It aimed to investigate how well children can identify and deal with privacy risks that are related to their use of tablet computers. The research process involved 12 focus group sessions that consisted of 29 children. The researchers used hypothetical scenarios featuring a cartoon character who experiences various online situations. Subsequently, the children were asked to express their opinions on these scenarios, discussing what they and the character should do.

4.3.6 Analyze Dataset. Datasets were analyzed in around 11.9% of the papers to identify patterns or trends and to gather more detailed information using other research methods. This step is often combined with other research methods, and it helps in finding themes to be able to use in other research methods. For example, Habib et al. [35] conducted a study to explore the patterns and motivations behind users' engagement with private browsing modes in web browsers. In the first step, they analyzed browsing data collected

from more than 450 participants. These users had given their consent to have their daily computing behavior monitored through software. This was followed by a survey to gain a better understanding of why people use private browsing for certain activities and whether they understand how it works.

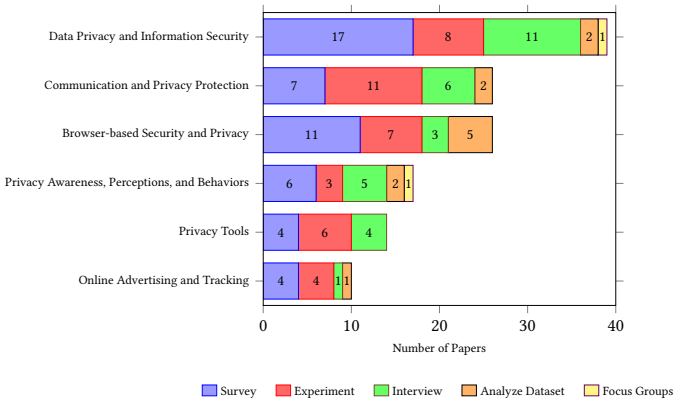

Figure 3: Cross-tab of topics and research methods

4.4 Research Methods within Research Topics

Our analysis also captured the intersection between the type of research method and research topics. The results (see Figure 3) show certain trends and preferences for approach within the different topics. Surveys are the most common method used, especially in data privacy and information security, where they are used around 44% of the time. Experimental methods are popular in areas like privacy tools (43%) and communication and privacy protection (42%). They are important because they allow for the testing of tools and strategies in a controlled environment. Interviews are another frequently used method, particularly in data privacy and information security (28%). They offer a more detailed and nuanced perspective, especially when individual experiences and perspectives are essential.

Dataset analysis was used less often and usually only when relevant to the topic and appropriate data is available. For example, it was more prominent in browser-based security and privacy (19%). Focus groups are not commonly used in any of the topics, possibly because they do not provide the depth or specificity required. Ultimately, researchers use specific methodologies tailored to the unique demands and specificities of each privacy-centric topic.

4.5 Study Characteristics

We also reviewed additional attributes of the different research methods found in the paper sample, as outlined in Table 4. This includes a detailed examination of critical factors such as whether the study was conducted in-person or online, synchronous or asynchronous (i.e., whether participants completed the study on in real-time with live communication with the researcher or if participants could independently complete the study without live researcher involvement), and whether it was performed in a group or individually.

4.5.1 In-person vs. Online. In terms of research methods, the Survey method was conducted entirely online, with all cases being carried out. The Experimental method mostly relied on online methods, with 87.2% of cases being conducted online and only 17.9% being carried out in-person. The Interview method showed a more balanced approach, with 66.7% of cases being conducted online and 33.3% in-person. All the Focus Groups were conducted in-person.

4.5.2 Synchronous vs. Asynchronous. The survey method used in the study was conducted asynchronously, allowing all participants to engage at their convenience. On the other hand, the experiment method was mostly asynchronous, with 89.7% of cases being asynchronous, whereas only 12.8% were synchronous. The interview method was predominantly synchronous, with 93.3% of cases being conducted in real-time, and only 6.7% being asynchronous. Both of the focus group cases were conducted in real-time, making them 100% synchronous.

4.5.3 Group vs. Individual. In the survey method, all studies were completed individually. Similarly, for the experiment method, the majority of cases (94.9%) were individual-based, with only 7.7% being conducted in a group setting. The interview method also showed a preference for individual sessions, with 90% being conducted individually and only 13.3% being group-based. As expected, focus groups were conducted in a group setting, representing 100% of the 2 total cases.

4.5.4 Number of Study Participants. The data presents clear trends in the number of participants across different research methods, with quantitative methods showing the median participant numbers, as can be seen in Table 5. Surveys, with a median of 393 participants, are particularly popular for gathering large-scale data. Surveys often aim to capture broad population-level insights, which necessitate higher participant counts to ensure statistical power and generalizability.

Also, experiments follow closely with a median of 390 participants, reflecting their frequent use in controlled empirical investigations. Experiments typically involve a controlled setup with a narrowly defined population to minimize variability and increase reliability. This focus often results in fewer extreme outliers compared to surveys, which might include very large participant counts (e.g., thousands in online surveys) for broad demographic insights. Consequently, while surveys can have a broader range, experiments maintain a more consistent participant count.

On the other hand, qualitative methods such as interviews and focus groups have considerably lower median participant numbers, 20 and 18, respectively. This is primarily because these methods are inherently time-intensive and cannot typically be conducted asynchronously. Both interviews and focus groups involve direct, real-time interaction between researchers and participants, which limits the number of participants that can feasibly be accommodated within the constraints of time and resources.

Additionally, these methods often result in extensive, detailed qualitative data that require time-intensive analysis, such as thematic coding or transcription, further limiting their scalability. For focus groups, the need for coordination among multiple participants in a single session adds an additional logistical challenge, contributing to their smaller participant numbers. This explains

their less frequent application and lower participant counts, with focus groups being utilized in only two out of six topics. In summary, the preference for quantitative methods like surveys and experiments is evident, as they dominate in participant numbers across most studies.

Research Method	Min-Max Bar
Survey	29 — 393 — 10212
Experiment	9 — 390 — 4594
Interview	9 — 20 — 67
Focus Groups	7 — 18 — 29

Table 5: Min-max bars representing the range of participant counts for each research method across all topics, with dots indicating the median values.

5 DISCUSSION

5.1 Analysis of Topics

Understanding the distribution of research topics provides valuable insight into the focus areas and potential gaps in the field of usable security and privacy (USP). This subsection examines the major themes of research and identifies trends, priorities, and areas needing further exploration. As illustrated in Table 2, the distribution of papers across different topics shows that a large portion of papers (30.7%) focus on *Data Privacy and Information Security*. This likely reflects the critical importance of protecting personal data in today's world, where data breaches can have serious effects on both individuals and organizations. The high number of studies highlights ongoing challenges like understanding how users handle passwords, share data, and spot phishing attempts. It also indicates a need to develop user-friendly solutions that improve security without making things too complicated.

In contrast, topics like *Privacy Tools* (9.9%) and *Online Advertising and Tracking* (6.9%) have received less attention. This difference raises questions about whether some important areas are being overlooked. For example, *Privacy Tools*—such as VPNs, encryption software, and privacy-focused browser add-ons—are key for protecting user data. The lower research focus here might not mean these tools are less important; it could be that studying how usable they are and why people do or don't use them is challenging. Many users find these tools complex or intrusive, which leads to low adoption rates. This suggests we need more research to make these tools easier to use and to understand what prevents people from using them.

Similarly, the smaller number of studies on *Online Advertising and Tracking* is notable given how common targeted advertising and tracking technologies are today. These practices raise significant privacy concerns, like collecting personal data without consent and profiling users. The lack of research might be because these tracking technologies are hard to study—they are always changing, and companies often hide them from users. There's a pressing need to clarify how these technologies work and to assess their impact on user privacy. This can help inform policies and lead to tools that help users manage their online footprints.

Figure 3 shows trends in using research methods across different topics in privacy studies. For instance, *surveys* are predominantly used in Data Privacy and Information Security, reflecting the method's strength in collecting large-scale quantitative data that can capture broad patterns and trends. *Surveys* allow researchers to gather data from a broad audience, making identify general opinions and behaviors. This approach is suitable for understanding the issues and concerns in *data privacy and information security*. Conversely, *surveys* are among the least used methods in the study of *privacy tools*. This indicates a reduced need for broad quantitative data, likely because the effectiveness and user interaction with *privacy tools* may require more hands-on exploration, which *surveys* are less equipped to handle.

On the other hand, *experiments* are generally employed more than *interviews* across various topics. However, *interviews* are utilized more extensively in the domains of *data privacy and information security*, as well as *privacy awareness, perceptions, and behaviors*. Interestingly, these are also the only two topics where *focus groups* were our review found examples of *focus groups* employed, perhaps further highlighting the value of qualitative methods for understanding user thinking in these topic areas. Using *interviews* and *focus groups* shows the need for in-depth, qualitative analysis to explore complex, subjective experiences and perceptions. *Focus groups*, in particular, bring the advantage of dynamic discussions, where participants can react to each other's perspectives, which is valuable for understanding deep or unspoken factors influencing privacy behaviors and perceptions. However, these methods were used less frequently overall in the paper sample—likely because quality *interviews* and *focus groups* are time-consuming to organize and conduct, and it can be challenging to manage and analyze the often complex qualitative data that results from them.

5.2 Analysis of Study Methods

Although *surveys*, *experiments*, and *interviews* are popular study methods, *focus groups* are less utilized, with only 1.9%, as shown in Table 4. One reason for this could be the challenge of coordinating and managing communication among a diverse group of experts or individuals at a specific time. However, *focus groups* have limitations in the ability to assess usability because people may not know what they want or need [52]. Additionally, online *focus groups* are difficult to keep confidential and may not be representative of the average user, and are time-consuming and expensive. However, it is essential to consider the benefits of *focus groups* which can give researchers valuable information and a deeper understanding of users' mental models. For example, [72] conducted *focus groups* with seven data deletion experts that helped them to categorize different topics to be discussed with users and used their thoughts as a baseline to compare with *interviews* that they did with users after that. While [130] utilized *focus groups* to understand children's mental models and privacy risks, which interactively gathered data that was not easily accessible through other research methods.

On the other hand, *surveys* with a 47.5% usage rate are commonly used in various research studies due to their ease of conduct and the reduced need for collaboration and control. *Surveys* can save time

	Survey	Experiment	Interview	Focus Groups	Analyze Dataset
Data Privacy and Information Security	[7], [109], [49], [94], [114], [95], [54], [81], [129], [47], [69], [51], [48], [133], [65], [8], [98]	[40], [103], [110], [24], [107], [119], [104], [60]	[106], [72], [67], [122], [78], [4], [60], [49], [94], [129], [98]	[72]	[94], [114]
Communication and Privacy Protection	[77], [22], [118], [62], [126], [127]	[58], [39], [5], [6], [70], [88], [131], [102], [59], [73], [12]	[87], [116], [112], [21], [4], [77]		[126], [127]
Browser-based Security and Privacy	[61], [76], [46], [64], [132], [97], [79], [90], [113], [75], [35]	[26], [11], [9], [86], [61], [108], [36]	[42], [90], [113]		[42], [75], [108], [36]
Privacy Awareness, Perceptions, and Behaviors	[41], [82], [17], [89], [85], [37]	[80], [53], [33]	[120], [84], [32], [41], [82]	[130]	[85], [37]
Privacy Tools	[19], [101], [100], [74]	[63], [99], [50], [115], [27], [20]	[19], [101], [63], [99]		
Online Advertising and Tracking	[16], [28], [38], [66]	[38], [105], [71], [56]	[56]		[66]

Table 6: Multidimensional summary of final 101 papers

and allow for the collection of a vast amount of information from a broad range of people. In survey research, most of the studies conducted tend to involve questionnaires rather than descriptive studies, according to Figure 2. While questionnaires are more accessible to create and administer, it might be a good idea to consider having users perform a task or a hypothetical scenario instead and then gather information from them such as in [81] which aimed to understand how users provide false information and tell privacy lies online by asking participants to imagine buying a movie ticket as part of a hypothetical task.

Descriptive studies could result in better insights since questionnaires often rely on self-reported data, which can be flawed and inaccurate, but by observing users' behaviors, researchers can get an understanding of how users interact and how their behaviors may change over time, leading to better research outcomes.

Although *surveys* and *experiments* are commonly used methods in many fields, analyzing datasets in conjunction with user studies is not widely utilized across all topics covered in this review. Given the potential benefits of *analyzing dataset* in understanding the problem and context before conducting a user study, this can have a significant impact. For instance, it is interesting to note that *analyzing dataset* is predominantly used in *browser-based security and privacy*, with 19% of researchers using it to qualitatively analyze users' online comments about Chrome's notification [42]. This data was then used to conduct *interviews* later. However, it is worth noting that none of the researchers utilized this method in *privacy tools*. This is a missed opportunity, as different types of online data from *privacy tools* like password managers, VPNs, or privacy nudges may be available for analysis, which could yield valuable insights.

Building on these observations about study methods and their applications, it is useful to compare our findings with prior reviews, such as Distler et al.'s research, to contextualize trends and differences over time. It is important to note that our review primarily focuses on topics related to online information disclosure, while Distler et al. [18] took a broader approach to papers in the field of USP employing human-subjects studies during the period preceding our own review. Although both reviews analyzed different study methods and topics, their objectives were different. Their analysis concentrates on the strategic choices made by researchers in representing risk in their studies, which can impact the study's design and yields, particularly in fields where understanding risk perception and behavior is essential. In contrast, our review aimed to categorize and compare specific research topics and methods, conducting cross-comparisons across different application areas and directly examining varied case studies to understand methodological patterns in the context of online privacy and security behaviors.

According to Distler et al.'s research, which reviewed papers from 2014–2018, *experiments* were the most commonly used method at 35%, followed by *interviews* and *surveys* at 13% and 12%, respectively. However, in our paper, from 2018 to 2023, *surveys* were found to be the most commonly used method at 47.5%, followed by *experiments* and *interviews* at 38.6% and 29.7%, respectively. Both *surveys* also noted that analyzing datasets and conducting *focus groups* were less commonly used methods. Focused groups were less utilized because they are less effective for creating realistic or controlled representations of security and privacy risks. Unlike experiments, which allow for precise manipulation of risk scenarios, or surveys, which can capture naturally occurring behaviors, focus groups often rely on shared discussions that may not align with the study's need for individual or measurable responses to risk.

Distler et al. [18] found that studies with descriptive methods often involved naturally occurring or mentioned risks, highlighting how risks were studied in prior research. This context helps frame the methodology and focus of current findings, particularly in understanding the relevance of risk representation to study objectives. This is because descriptive methods usually provide less opportunity for risk simulation and are better suited for evaluating real-life risks or mentioned risks using *interviews* or *surveys*. Our analysis found that *data privacy and information security* emerged as the leading topic with the most papers, which often focuses on descriptive methods due to its emphasis on understanding users' behavior when sharing personal data, where naturally occurring risks are more relevant. In contrast, experimental methods are more prevalent in areas such as *communication and privacy protection* and *privacy tools*, as these topics benefit from controlled environments to simulate risks and test user responses to tools and messaging platforms. This aligns with Distler et al., who highlighted the importance of experimental setups for studying risk simulation effectively in these contexts.

5.3 Application Areas within Different Topics and Methods

Understanding the application areas of research topics and methods bridges theoretical insights with practical implementations. This section examines how various empirical studies on online information disclosure are applied across specific software platforms and contexts. While 41.5% of papers from the reviewed sample focused on nonspecific application areas, as shown in Table 3, diving into

specific sections that provide more details for each context might also be essential. Differences in types of applications and technologies will logically translate to different forms of privacy risks, as demonstrated in Figure 1. While studies with more generalized concepts are undoubtedly useful in covering widely applicable insights that can apply to many application contexts, the general approach also risks missing out on key insights into the unique risks posed by more specific applications.

It is therefore critical to also conduct targeted, application-specific research, and the results of our review suggest more attention to key areas may be warranted. For example, despite the increasing use of mobile apps, common adoption of smartphones, and expanding use of mobile applications for services, Figure 1 shows research of mobile apps received less attention during the sampled period. Mobile apps tend to collect and use a significant amount of personal data, but they do so in different ways compared to non-mobile apps.

Similarly, social media is a significant part of modern life for many people, which received a relatively small amount of focus overall—and the analysis did not yield any direct examples of the intersection between specific *social media* applications and the topic of *online advertising and tracking*. Understanding the specific risks within these contexts is essential if we want to develop targeted privacy solutions.

These examples demonstrate the value of considering the focus of different application areas, as a broad coverage with both specific and nonspecific applications is important for developing more nuanced privacy protections. Within application categories, the focus on browser applications was high (21.7% or 22 papers) compared to other specific areas such as social media and mobile. As almost every person uses these applications, it is crucial to pay as much attention to them as much as other areas and mitigate the risks associated with their usage. It is worth noting that email is another application area that had relatively lower overall focus in sampled user studies. This is possibly due to the longer history of email usage in daily life, and research advancements in phishing algorithms can also filter out many untrustworthy emails by taking advantage of non-expert users [118]. However, attention to this area is still necessary as email is an essential communication tool for most people.

5.4 Recent developments in generative AI and data disclosure

Recent work from 2024 and 2025 further highlights how unintentional disclosure risks are evolving in the context of generative AI systems and associated policy debates [2, 15, 34, 124]. Several empirical and data-driven studies have examined how people disclose personal information to conversational models and how they reason about privacy in these interactions. For example, studies of ChatGPT users document how people share sensitive details, struggle to understand data retention and reuse, and navigate trade-offs between convenience and privacy when using the system in everyday tasks and problem-solving [2, 124]. Other work focuses on professional and organizational settings, showing how the use of generative AI tools at work can create networked privacy risks when individuals input information about colleagues, clients, or internal processes, and how these disclosures interact with workplace norms and policies [123]. Large-scale surveys and interviews have also begun to map public perceptions of privacy in interactions with large language models, including concerns about training data, secondary use of prompts, and uncertainty over who can access generated content[15].

In parallel, there has been rapid development in policy and governance responses that directly address data disclosure in AI systems. Surveys of organizational practice show that many companies are restricting or banning the use of generative AI tools because employees have reported past disclosure of non-public data to these services, and decision-makers remain unsure how providers handle such information [34]. Together, these developments demonstrate that generative AI tools have rapidly become a significant setting for unintentional information disclosure, and that questions about data use, retention, and accountability are now central to both empirical research and policy discussions. Future empirical work should investigate how users understand these systems, how interface design shapes disclosure decisions, and how regulatory expectations align with actual user behavior.

6 LIMITATIONS AND FUTURE WORK

The analysis presented here is based on only a limited number of papers in USP field involving human-subject studies. At USP, many areas use human subjects, which can provide a large sample size, as demonstrated in studies such as Distler et al. [18], to evaluate the impact of different empirical methods. However, this paper narrows the focus to online information disclosure, primarily concerning scenarios where human decision-making and understanding can affect privacy. As we are confident that this topic is important to evaluate, the existing literature and taxonomies lacks a categorization of topics in this area due to its narrow focus. Therefore, our sub-topic extraction might not align with past literature but can be used as a starting point in this area. As USP papers published in journals were limited, we did not consider them a major publication venue and were missing from our sample.

As described previously, our review concentrates on the methods used to study online information disclosure. This includes cases where users may not be fully aware of the risks, which often leads to unintentional information disclosure. As a result, we have excluded topics such as encryption, authentication, and IoT/mobile security, which directly address these types of risks. Nonetheless, we acknowledge that some empirical research in these areas may have been inadvertently omitted from our review.

Also, although our search strategy included six major digital libraries and covered a wide range of venues, our scope focused primarily on conference proceedings rather than on a full coverage of journal publications. This decision reflects the distribution of research in this area, as preliminary screening showed that a large share of empirical studies on unintentional disclosure are published in conference venues, particularly within the human computer interaction and privacy communities. Journal publications in this domain tend to include fewer human subjects studies or focus on technical or policy oriented analyses that fall outside the scope of our research questions. While this choice allowed us to maintain methodological consistency, it may have excluded relevant articles

from major journals. We therefore acknowledge this as a limitation and encourage future work to incorporate a broader range of publications.

Moreover, our review identifies several limitations in the current literature that point to promising opportunities for future research. A clear imbalance exists in the methodological landscape, with most studies relying on descriptive approaches such as surveys and interviews, while longitudinal and real world methods remain rare. Because unintentional disclosure often develops gradually as users become accustomed to interfaces and warning mechanisms, future work should explore longer term and in the wild behavior to capture how disclosure patterns change over time. In addition, the distribution of application domains shows that mobile platforms and social media receive far less empirical attention than browsers or general online contexts, even though mobile and social applications dominate everyday digital interaction. Future research would benefit from examining disclosure events that arise through mobile permissions, background data sharing, messaging features, and tracking across applications, all of which represent situations where users frequently disclose information without realizing it.

Our analysis also reveals topics that remain under investigated despite their growing relevance. Privacy tools and online advertising and tracking appear far less often in the empirical literature than other topics, even though they involve high frequency collection and inference of personal data. These areas would benefit from studies that address how users understand and manage risks that arise from profiling and third party aggregation. Finally, although experimental studies do appear in the literature, many rely on simplified or hypothetical scenarios rather than realistic tasks or interfaces. Future work could strengthen the evidence base by using more ecologically valid experimental designs or mixed methodological approaches that combine behavioral data with qualitative insights in order to better capture user intentions, mental models, and disclosure awareness during actual interaction.

7 CONCLUSION

We systematically reviewed 101 papers in USP-related research dealing with online information disclosure as seen in Table 6, which allowed us to categorize each paper based on research methods, topics, and application areas. We looked into the intersection of different categorizations, such as using study methods in topics and application areas across topics, to reveal how researchers utilize various methods to gain insight across other areas. The review explored various methods used by researchers to gain insight across different areas and concluded that descriptive research methods were preferred over experimental methods. Surveys in questionnaire structure were particularly favored over descriptive formats that required users to perform a task. Surveys in questionnaire structure were particularly favored over descriptive formats that required users to perform a task. Additionally, privacy tools and email in application areas seem to receive less attention, indicating that there is potential for improvement in the development of tools that can enhance privacy protection, particularly in the context of phishing scenarios. The researchers should pay attention to the sensitive topic of online advertising and tracking much more. This issue has the potential to put many aspects of privacy and security in danger. It can allow attackers to infer sensitive information and even execute location-related attacks.

8 DISCLOSURE STATEMENT

No potential conflict of interest was reported by the author(s).

REFERENCES

[1] Ruba Abu-Salma, M Angela Sasse, Joseph Bonneau, Anastasia Danilova, Alena Naiakshina, and Matthew Smith. 2017. Obstacles to the adoption of secure communication tools. In *2017 IEEE Symposium on Security and Privacy (SP)*. IEEE, 137–153.

[2] Shahad Alkamli and Reham Alabduljabbar. 2024. Understanding privacy concerns in ChatGPT: A data-driven approach with LDA topic modeling. *Heliyon* 10, 20 (2024).

[3] Hazim Almuhimedi, Adrienne Porter Felt, Robert W Reeder, and Sunny Consolvo. 2014. Your reputation precedes you: History, reputation, and the chrome malware warning. In *10th Symposium On Usable Privacy and Security (SOUPS 2014)*. 113–128.

[4] Abdulmajeed Alqhatani and Heather Richter Lipford. 2019. {"There} is nothing that I need to keep {secret"}: Sharing Practices and Concerns of Wearable Fitness Data. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. 421–434.

[5] Kholoud Althobaiti, Nicole Meng, and Kami Vaniea. 2021. I don't need an expert! Making URL phishing features human comprehensible. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–17.

[6] Mary Jean Amon, Rakibul Hasan, Kurt Hugenberg, Bennett I Bertenthal, and Apu Kapadia. 2020. Influencing photo sharing decisions on social media: A case of paradoxical findings. In *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, 1350–1366.

[7] Patricia Arias-Cabarcos, Saina Khalili, and Thorsten Strufe. 2022. 'Surprised, Shocked, Worried': User Reactions to Facebook Data Collection from Third Parties. *arXiv preprint arXiv:2209.08048* (2022).

[8] David G Balash, Xiaoyuan Wu, Miles Grant, Irwin Reyes, and Adam J Aviv. 2022. Security and Privacy Perceptions of {Third-Party} Application Access for Google Accounts. In *31st USENIX Security Symposium (USENIX Security 22)*. 3397–3414.

[9] Matthew Bernhard, Jonathan Sharman, Claudia Ziegler Acemyan, Philip Kortum, Dan S Wallach, and J Alex Halderman. 2019. On the usability of https deployment. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–10.

[10] Bhaveer Bhana and Stephen Flowerday. 2020. Passphrase and keystroke dynamics authentication: Usable security. *Computers & Security* 96 (2020), 101925.

[11] Elijah Robert Bouma-Sims, Megan Li, Yanzi Lin, Adia Sakura-Lemessy, Alexandra Nisenoff, Ellie Young, Eleanor Birrell, Lorrie Faith Cranor, and Hana Habib. 2023. A US-UK Usability Evaluation of Consent Management Platform Cookie Consent Interface Design on Desktop and Mobile. In *Proceedings of the 2@inproceedingsbernhard2019usability, title=On the usability of https deployment, author=Bernhard, Matthew and Sharman, Jonathan and Acemyan, Claudia Ziegler and Kortum, Philip and Wallach, Dan S and Halderman, J Alex, booktitle=Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, pages=1–10, year=2019 023 CHI Conference on Human Factors in Computing Systems*. 1–36.

[12] Vanessa Bracamonte, Sebastian Pape, and Sascha Loebner. 2022. All apps do this": Comparing privacy concerns towards privacy tools and non-privacy tools for social media content. *Proceedings on Privacy Enhancing Technologies* 3 (2022), 57–78.

[13] Cristian Bravo-Lillo, Saranga Komanduri, Lorrie Faith Cranor, Robert W Reeder, Manya Sleeper, Julie Downs, and Stuart Schechter. 2013. Your attention please: Designing security-decision UIs to make genuine risks harder to ignore. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*. 1–12.

[14] Hongliang Chen, Christopher E Beaudoin, and Traci Hong. 2017. Securing online privacy: An empirical test on Internet scam victimization, online privacy concerns, and privacy protection behaviors. *Computers in human behavior* 70 (2017), 291–302.

[15] Yubin Choi, Assem Zhunis, Wenchao Dong, Joseph Seering, Sangchul Park, Meeyoung Cha, and Hyojin Chin. 2025. Privacy disclosure to large language models: A large-scale study on awareness, benefits, and concerns in health contexts across three countries. *Computers in Human Behavior Reports* 20 (2025), 100841.

[16] Kovila PL Coopamootoo, Maryam Mehrnezhad, and Ehsan Toreini. 2022. " I feel invaded, annoyed, anxious and I may protect myself": Individuals' Feelings about Online Tracking and their Protective Behaviour across Gender and Country. In *31st USENIX Security Symposium (USENIX Security 22)*. 287–304.

[17] Sauvik Das, Laura A Dabbish, and Jason I Hong. 2019. A typology of perceived triggers for {End-User} security and privacy behaviors. In *Fifteenth Symposium*

on Usable Privacy and Security (SOUPS 2019). 97–115.

[18] Verena Distler, Matthias Fassl, Hana Habib, Katharina Krombholz, Gabriele Lenzini, Carine Lallemand, Lorrie Faith Cranor, and Vincent Koenig. 2021. A systematic literature review of empirical methods and risk representation in usable privacy and security research. *ACM Transactions on Computer-Human Interaction (TOCHI)* 28, 6 (2021), 1–50.

[19] Agnieszka Dutkowska-Zuk, Austin Hounsel, Amy Morrill, Andre Xiong, Marshini Chetty, and Nick Feamster. 2022. How and why people use virtual private networks. In *31st USENIX Security Symposium (USENIX Security 22)*. 3451–3465.

[20] Nico Ebert, Kurt Alexander Ackermann, and Björn Scheppler. 2021. Bolder is better: Raising user awareness through salient and concise privacy notices. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–12.

[21] Nico Ebert, Tim Geppert, Joanna Strycharz, Melanie Knieps, Michael Hönig, and Elke Brucker-Kley. 2023. Creative beyond TikToks: investigating Adolescents' Social privacy management on TikTok. *arXiv preprint arXiv:2301.11600* (2023).

[22] Pardis Emami-Naeini, Tiona Francisco, Tadayoshi Kohno, and Franziska Roesner. 2021. Understanding Privacy Attitudes and Concerns Towards Remote Communications During the {COVID-19} Pandemic. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*. 695–714.

[23] Michael Fagan and Mohammad Maifi Hasan Khan. 2016. Why do they do what they do?: A study of what motivates users to (not) follow computer security advice. In *Twelfth symposium on usable privacy and security (SOUPS 2016)*. 59–75.

[24] Florian M Farke, David G Balash, Maximilian Golla, Markus Dürmuth, and Adam J Aviv. 2021. Are privacy dashboards good for end users? Evaluating user perceptions and reactions to Google's My Activity. In *30th USENIX Security Symposium (USENIX Security 21)*. 483–500.

[25] Adrienne Porter Felt, Robert W Reeder, Alex Ainslie, Helen Harris, Max Walker, Christopher Thompson, Mustafa Embre Acer, Elisabeth Morant, and Sunny Consolvo. 2016. Rethinking connection security indicators. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. 1–14.

[26] Alisa Frik, Amelia Haviland, and Alessandro Acquisti. 2020. The Impact of {Ad-Blockers} on Product Search and Purchase Behavior: A Lab Experiment. In *29th USENIX Security Symposium (USENIX Security 20)*. 163–179.

[27] Alisa Frik, Nathan Malkin, Marian Harbach, Eyal Peer, and Serge Egelman. 2019. A promise is a promise: The effect of commitment devices on computer security intentions. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–12.

[28] Sandra Gabriele and Sonia Chiasson. 2020. Understanding fitness tracker users' security and privacy knowledge, attitudes and behaviours. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–12.

[29] Kevin Gallagher, Sameer Patil, and Nasir Memon. 2017. New Me: Understanding Expert and {Non-Expert} Perceptions and Usage of the Tor Anonymity Network. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. 385–398.

[30] Simson Garfinkel. 1995. *PGP: pretty good privacy.* " O'Reilly Media, Inc.".

[31] Simson Garfinkel and Heather Richter Lipford. 2014. *Usable security: History, themes, and challenges*. Morgan & Claypool Publishers.

[32] Nina Gerber and Karola Marky. 2022. The Nerd Factor: The Potential of {S&P} Adepts to Serve as a Social Resource in the User's Quest for More Secure and {Privacy-Preserving} Behavior. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*. 57–76.

[33] Nina Gerber, Benjamin Reinheimer, and Melanie Volkamer. 2019. Investigating People's Privacy Risk Perception. *Proc. Priv. Enhancing Technol.* 2019, 3 (2019), 267–288.

[34] Maanak Gupta, CharanKumar Akiri, Kshitiz Aryal, Eli Parker, and Lopamudra Praharaj. 2023. From chatgpt to threatgpt: Impact of generative ai in cybersecurity and privacy. *IEEE access* 11 (2023), 80218–80245.

[35] Hana Habib, Jessica Colnago, Vidya Gopalakrishnan, Sarah Pearman, Jeremy Thomas, Alessandro Acquisti, Nicolas Christin, and Lorrie Faith Cranor. 2018. Away from prying eyes: Analyzing usage and understanding of private browsing. In *Fourteenth symposium on usable privacy and security (SOUPS 2018)*. 159–175.

[36] Hana Habib, Megan Li, Ellie Young, and Lorrie Cranor. 2022. "Okay, whatever": An Evaluation of Cookie Consent Interfaces. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*. 1–27.

[37] Catherine Han, Irwin Reyes, Álvaro Feal, Joel Reardon, Primal Wijesekera, Narseo Vallina-Rodriguez, Amit Elazar, Kenneth A Bamberger, and Serge Egelman. 2020. The price is (not) right: Comparing privacy in free and paid apps. *Proceedings on Privacy Enhancing Technologies* 2020, 3 (2020).

[38] Julia Hanson, Miranda Wei, Sophie Veys, Matthew Kugler, Lior Strahilevitz, and Blase Ur. 2020. Taking Data Out of Context to Hyper-Personalize Ads: Crowdworkers' Privacy Perceptions and Decisions to Disclose Private Information. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–13.

[39] Rakibul Hasan, Bennett I Bertenthal, Kurt Hugenberg, and Apu Kapadia. 2021. Your photo is so funny that i don't mind violating your privacy by sharing it: effects of individual humor styles on online photo-sharing behaviors. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–14.

[40] Rakibul Hasan, Eman Hassan, Yifang Li, Kelly Caine, David J Crandall, Roberto Hoyle, and Apu Kapadia. 2018. Viewer experience of obscuring scene elements in photos to enhance privacy. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. 1–13.

[41] Rakibul Hasan, Rebecca Weil, Rudolf Siegel, and Katharina Krombholz. 2023. A Psychometric Scale to Measure Individuals' Value of Other People's Privacy (VOPP). In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. 1–14.

[42] Yue Huang, Borke Obada-Obieh, and Konstantin Beznosov. 2022. Users' Perceptions of Chrome Compromised Credential Notification. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*. 155–174.

[43] Giovanni Iachello, Jason Hong, et al. 2007. End-user privacy in human–computer interaction. *Foundations and Trends® in Human–Computer Interaction* 1, 1 (2007), 1–137.

[44] Danielle Jacobs and Troy McDaniel. 2022. A survey of user experience in usable security and privacy research. In *International Conference on Human-Computer Interaction*. Springer, 154–172.

[45] Tom N Jagatic, Nathaniel A Johnson, Markus Jakobsson, and Filippo Menczer. 2007. Social phishing. *Commun. ACM* 50, 10 (2007), 94–100.

[46] Ankit Kariryaa, Gian-Luca Savino, Carolin Stellmacher, and Johannes Schöning. 2021. Understanding users' knowledge about the privacy and security of browser extensions. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*. 99–118.

[47] Sowmya Karunakaran, Kurt Thomas, Elie Bursztein, and Oxana Comanescu. 2018. Data breaches: User comprehension, expectations, and concerns with handling exposed data. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. 217–234.

[48] Mohammad Taha Khan, Maria Hyun, Chris Kanich, and Blase Ur. 2018. Forgotten but not gone: Identifying the need for longitudinal data management in cloud storage. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. 1–12.

[49] Mohammad Taha Khan, Christopher Tran, Shubham Singh, Dimitri Vasilkov, Chris Kanich, Blase Ur, and Elena Zheleva. 2021. Helping users automatically find and manage sensitive, expendable files in cloud storage. In *30th USENIX Security Symposium (USENIX Security 21)*. 1145–1162.

[50] Agnieszka Kitkowska, Mark Warner, Yefim Shulman, Erik Wästlund, and Leonardo A Martucci. 2020. 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)*. 437–456.

[51] Jacob Leon Kröger, Leon Gellrich, Sebastian Pape, Saba Rebecca Brause, and Stefan Ullrich. 2022. Personal information inference from voice recordings: User awareness and privacy concerns. *Proc. Priv. Enhancing Technol.* 2022, 1 (2022), 6–27.

[52] Richard A Krueger. 2014. *Focus groups: A practical guide for applied research*. Sage publications.

[53] Markus Langer, Rudolf Siegel, Michael Schilling, Tim Hunsicker, and Cornelius J König. 2022. An open door may tempt a saint: Examining situational and individual determinants of privacy-invading behavior. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*. 407–426.

[54] Celine Latulipe, Ronnie Dsouza, and Murray Cumbers. 2022. Unofficial Proxies: How Close Others Help Older Adults with Banking. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*. 1–13.

[55] Jonathan Lazar, Jinjuan Heidi Feng, and Harry Hochheiser. 2017. *Research methods in human-computer interaction*. Morgan Kaufmann.

[56] Hao-Ping Hank Lee, Jacob Logas, Stephanie Yang, Zhouyu Li, Nata Barbosa, Yang Wang, and Sauvik Das. 2023. When and Why Do People Want Ad Targeting Explanations? Evidence from a Four-Week, Mixed-Methods Field Study. In *2023 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2903–2920.

[57] Enze Liu, Amanda Nakanishi, Maximilian Golla, David Cash, and Blase Ur. 2019. Reasoning analytically about password-cracking software. In *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, 380–397.

[58] Enze Liu, Lu Sun, Alex Bellon, Grant Ho, Geoffrey M Voelker, Stefan Savage, and Imani NS Munyaka. 2023. Understanding the Viability of Gmail's Origin Indicator for Identifying the Sender. In *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)*. 77–95.

[59] Gary Liu and Nathan Malkin. 2022. Effects of privacy permissions on user choices in voice assistant app stores. *Proc. Privacy Enhancing Technol.* 2022, 4 (2022), 421–439.

[60] Yijing Liu, Yan Jia, Qingyin Tan, Zheli Liu, and Luyi Xing. 2022. How Are Your Zombie Accounts? Understanding Users' Practices and Expectations on Mobile App Account Deletion. In *31st USENIX Security Symposium (USENIX Security 22)*. 863–880.

[61] Max Maass, Alina Stöver, Henning Pridöhl, Sebastian Bretthauer, Dominik Herrmann, Matthias Hollick, and Indra Spiecker. 2021. Effective notification campaigns on the web: A matter of trust, framing, and support. In *30th USENIX*

Security Symposium (USENIX Security 21). 2489–2506.
[62] Nathan Malkin, Joe Deatrick, Allen Tong, Primal Wijesekera, Serge Egelman, and David Wagner. 2019. Privacy attitudes of smart speaker users. *Proceedings on Privacy Enhancing Technologies* 2019, 4 (2019).
[63] Hiroaki Masaki, Kengo Shibata, Shui Hoshino, Takahiro Ishihama, Nagayuki Saito, and Koji Yatani. 2020. Exploring nudge designs to help adolescent sns users avoid privacy and safety threats. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–11.
[64] Arunesh Mathur, Jessica Vitak, Arvind Narayanan, and Marshini Chetty. 2018. Characterizing the Use of {Browser-Based} Blocking Extensions To Prevent Online Tracking. In *Fourteenth symposium on usable privacy and security (SOUPS 2018)*. 103–116.
[65] Peter Mayer, Yixin Zou, Florian Schaub, and Adam J Aviv. 2021. " Now I'm a bit {angry:}" Individuals' Awareness, Perception, and Responses to Data Breaches that Affected Them. In *30th USENIX Security Symposium (USENIX Security 21)*. 393–410.
[66] Maryam Mehrnezhad, Kovila Coopamootoo, and Ehsan Toreini. 2022. How can and would people protect from online tracking? *Proceedings on Privacy Enhancing Technologies* 1 (2022), 105–125.
[67] Helena M Mentis, Galina Madjaroff, and Aaron K Massey. 2019. Upside and downside risk in online security for older adults with mild cognitive impairment. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–13.
[68] Melita Milenković and Goran Vojković. 2025. Implementation of Regulation (EU) 2024/1183 in Higher Education in the Republic of Croatia. In *2025 MIPRO 48th ICT and Electronics Convention*. IEEE, 1642–1647.
[69] Mohsen Minaei, Mainack Mondal, and Aniket Kate. 2022. Empirical Understanding of Deletion Privacy: Experiences, Expectations, and Measures. In *31st USENIX Security Symposium (USENIX Security 22)*. 3415–3432.
[70] Jaron Mink, Licheng Luo, Natã M Barbosa, Olivia Figueira, Yang Wang, and Gang Wang. 2022. {DeepPhish}: Understanding User Trust Towards Artificially Generated Profiles in Online Social Networks. In *31st USENIX Security Symposium (USENIX Security 22)*. 1669–1686.
[71] Jaron Mink, Amanda Rose Yuile, Uma Pal, Adam J Aviv, and Adam Bates. 2022. Users Can Deduce Sensitive Locations Protected by Privacy Zones on Fitness Tracking Apps. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*. 1–21.
[72] Ambar Murillo, Andreas Kramm, Sebastian Schnorf, and Alexander De Luca. 2018. " If I press delete, it's gone"-User Understanding of Online Data Deletion and Expiration. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. 329–339.
[73] Moses Namara, Henry Sloan, and Bart P Knijnenburg. 2021. The effectiveness of adaptation methods in improving user engagement and privacy protection on social network sites. (2021).
[74] Moses Namara, Daricia Wilkinson, Kelly Caine, and Bart P Knijnenburg. 2020. Emotional and practical considerations towards the adoption and abandonment of vpns as a privacy-enhancing technology. (2020).
[75] Alexandra Nisenoff, Arthur Borem, Madison Pickering, Grant Nakanishi, Maya Thumpasery, and Blase Ur. 2023. Defining "Broken": User Experiences and Remediation Tactics When Ad-Blocking or Tracking-Protection Tools Break a Website's User Experience. In *Proceedings of the 32nd USENIX Security Symposium*.
[76] Alexandra Nisenoff, Ranya Sharma, and Nick Feamster. 2023. User Awareness and Behaviors Concerning Encrypted {DNS} Settings in Web Browsers. In *32nd USENIX Security Symposium (USENIX Security 23)*. 3117–3133.
[77] Norbert Nthala and Ivan Flechais. 2018. Informal support networks: an investigation into home data security practices. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. 63–82.
[78] Borke Obada-Obieh, Yue Huang, and Konstantin Beznosov. 2020. The burden of ending online account sharing. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–13.
[79] Gaston Pugliese, Christian Riess, Freya Gassmann, and Zinaida Benenson. 2020. Long-Term Observation on Browser Fingerprinting: Users' Trackability and Perspective. *Proc. Priv. Enhancing Technol.* 2020, 2 (2020), 558–577.
[80] Emilee Rader. 2023. Data Privacy and Pluralistic Ignorance. In *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)*. 457–471.
[81] Kopo M Ramokapane, Gaurav Misra, Jose Such, and Sören Preibusch. 2021. Truth or dare: Understanding and predicting how users lie and provide untruthful data online. In *Proceedings of the 2021 CHI conference on human factors in computing systems*. 1–15.
[82] Hirak Ray, Flynn Wolf, Ravi Kuber, and Adam J Aviv. 2020. "Warn Them" or "Just Block Them"?: Investigating Privacy Concerns Among Older and Working Age Adults. *UMBC Student Collection* (2020).
[83] Paulo C Realpe, Cesar A Collazos, Julio Hurtado, and Antoni Granollers. 2015. Towards an integration of usability and security for user authentication. In *Proceedings of the XVI International Conference on Human Computer Interaction*. 1–6.
[84] Elissa M Redmiles. 2019. " Should I Worry?" A Cross-Cultural Examination of Account Security Incident Response. In *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, 920–934.
[85] Elissa M Redmiles, Noel Warford, Amritha Jayanti, Aravind Koneru, Sean Kross, Miraida Morales, Rock Stevens, and Michelle L Mazurek. 2020. A comprehensive quality evaluation of security and privacy advice on the web. In *29th USENIX Security Symposium (USENIX Security 20)*. 89–108.
[86] Robert W Reeder, Adrienne Porter Felt, Sunny Consolvo, Nathan Malkin, Christopher Thompson, and Serge Egelman. 2018. An experience sampling study of user reactions to browser warnings in the field. In *Proceedings of the 2018 CHI conference on human factors in computing systems*. 1–13.
[87] Jake Reichel, Fleming Peck, Mikako Inaba, Bisrat Moges, Brahmnoor Singh Chawla, and Marshini Chetty. 2020. 'I have too much respect for my elders': Understanding South African Mobile Users' Perceptions of Privacy and Current Behaviors on Facebook and {WhatsApp}. In *29th USENIX Security Symposium (USENIX Security 20)*. 1949–1966.
[88] Benjamin Reinheimer, Lukas Aldag, Peter Mayer, Mattia Mossano, Reyhan Duezguen, Bettina Lofthouse, Tatiana Von Landesberger, and Melanie Volkamer. 2020. An investigation of phishing awareness and education over time: When and how to best remind users. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. 259–284.
[89] Thea Riebe, Tom Biselli, Marc-André Kaufhold, and Christian Reuter. 2023. Privacy Concerns and Acceptance Factors of OSINT for Cybersecurity: A Representative Survey. *Proceedings on Privacy Enhancing Technologies* 1 (2023), 477–493.
[90] Elsa Rodríguez, Radu Anghel, Simon Parkin, Michel van Eeten, and Carlos Gañán. 2023. Two Sides of the Shield: Understanding Protective {DNS} adoption factors. In *32nd USENIX Security Symposium (USENIX Security 23)*. USENIX Association.
[91] M Angela Sasse and Ivan Flechais. 2005. Usable security: Why do we need it? How do we get it? O'Reilly.
[92] Max Sauer, Sascha Alpers, and Christoph Becker. 2023. Comparison of methods for analyzing the correlation of user experience and information security. In *Proceedings of the 2023 5th International Conference on Software Engineering and Development*. 8–16.
[93] Rachelle Sellung and Michael Kubach. 2023. Research on User experience for digital identitywallets: state-of-the-art and recommendations. In *Open Identity Summit 2023*. Gesellschaft für Informatik eV, 39–50.
[94] Bingyu Shen, Lili Wei, Chengcheng Xiang, Yudong Wu, Mingyao Shen, Yuanyuan Zhou, and Xinxin Jin. 2021. Can systems explain permissions better? understanding users' misperceptions under smartphone runtime permission model. In *30th USENIX Security Symposium (USENIX Security 21)*. 751–768.
[95] Camelia Simoiu, Joseph Bonneau, Christopher Gates, and Sharad Goel. 2019. " I was told to buy a software or lose my computer. I ignored it": A study of ransomware. In *Fifteenth symposium on usable privacy and security (SOUPS 2019)*. 155–174.
[96] Madeleine Sjöholm. 2023. Designing a Trustworthy EU Digital Identity Wallet: A study of user needs and preferences.
[97] Daniel Smullen, Yaxing Yao, Yuanyuan Feng, Norman Sadeh, Arthur Edelstein, and Rebecca Weiss. 2021. Managing potentially intrusive practices in the browser: A user-centered perspective. *UMBC Faculty Collection* (2021).
[98] Jonah Stegman, Patrick J Trottier, Caroline Hillier, Hassan Khan, and Mohammad Mannan. 2022. "My Privacy for their Security": Employees' Privacy Perspectives and Expectations when using Enterprise Security Software. *arXiv preprint arXiv:2209.11878* (2022).
[99] Peter Story, Daniel Smullen, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. 2020. From intent to action: Nudging users towards secure mobile payments. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. 379–415.
[100] Peter Story, Daniel Smullen, Yaxing Yao, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. 2021. Awareness, adoption, and misconceptions of web privacy tools. *UMBC Faculty Collection* (2021).
[101] Alina Stöver, Sara Hahn, Felix Kretschmer, and Nina Gerber. 2023. Investigating How Users Imagine Their Personal Privacy Assistant. *Proc. Priv. Enhancing Technol* 2 (2023), 384–402.
[102] Christian Stransky, Dominik Wermke, Johanna Schrader, Nicolas Huaman, Yasemin Acar, Anna Lena Fehlhaber, Miranda Wei, Blase Ur, and Sascha Fahl. 2021. On the Limited Impact of Visualizing Encryption: Perceptions of {E2E} Messaging Security. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*. 437–454.
[103] S Shyam Sundar and Jinyoung Kim. 2019. Machine heuristic: When we trust computers more than humans with our personal information. In *Proceedings of the 2019 CHI Conference on human factors in computing systems*. 1–9.
[104] S Shyam Sundar, Jinyoung Kim, Mary Beth Rosson, and Maria D Molina. 2020. Online privacy heuristics that predict information disclosure. In *Proceedings of the 2020 CHI conference on human factors in computing systems*. 1–12.
[105] Mohammad Tahaei, Alisa Frik, and Kami Vaniea. 2021. Deciding on personalized ads: Nudging developers about user privacy. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*. 573–596.

[106] Kejsi Take, Kevin Gallagher, Andrea Forte, Damon McCoy, and Rachel Greenstadt. 2022. "it feels like whack-a-mole": User experiences of data removal from people search websites. *Proceedings on Privacy Enhancing Technologies* 3 (2022), 159–178.
[107] Arnout Terpstra, Alwin De Rooij, and Alexander Schouten. 2023. Online Proctoring: Privacy Invasion or Study Alleviation? Discovering Acceptability Using Contextual Integrity. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. 1–20.
[108] Christopher Thompson, Martin Shelton, Emily Stark, Maximilian Walker, Emily Schechter, and Adrienne Porter Felt. 2019. The web's identity crisis: understanding the effectiveness of website identity indicators. In *28th USENIX Security Symposium (USENIX Security 19)*. 1715–1732.
[109] Jan Tolsdorf, Delphine Reinhardt, and Luigi Lo Iacono. 2022. Employees' privacy perceptions: exploring the dimensionality and antecedents of personal data sensitivity and willingness to disclose. *Proceedings on Privacy Enhancing Technologies* 2 (2022), 68–94.
[110] Ehsan Ul Haque, Mohammad Maifi Hasan Khan, and Md Abdullah Al Fahim. 2023. The Nuanced Nature of Trust and Privacy Control Adoption in the Context of Google. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. 1–23.
[111] Blase Ur, Felicia Alfieri, Maung Aung, Lujo Bauer, Nicolas Christin, Jessica Colnago, Lorrie Faith Cranor, Henry Dixon, Pardis Emami Naeini, Hana Habib, et al. 2017. Design and evaluation of a data-driven password meter. In *Proceedings of the 2017 chi conference on human factors in computing systems*. 3775–3786.
[112] Warda Usman, Jackie Hu, McKynlee Wilson, and Daniel Zappala. 2023. Distrust of big tech and a desire for privacy: Understanding the motivations of people who have voluntarily adopted secure email. In *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)*. 473–490.
[113] Christine Utz, Sabrina Amft, Martin Degeling, Thorsten Holz, Sascha Fahl, and Florian Schaub. 2022. Privacy Rarely Considered: Exploring Considerations in the Adoption of Third-Party Services by Websites. *arXiv preprint arXiv:2203.11387* (2022).
[114] Dirk Van Der Linden, Matthew Edwards, Irit Hadar, and Anna Zamansky. 2020. Pets without PETs: on pet owners' under-estimation of privacy concerns in pet wearables. *Proceedings on Privacy Enhancing Technologies* 2020, 1 (2020), 143–164.
[115] Anthony Vance, David Eargle, Jeffrey L Jenkins, C Brock Kirwan, and Bonnie Brinton Anderson. 2019. The fog of warnings: how non-essential notifications blur with security warnings. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. 407–420.
[116] Leijie Wang, Ruotong Wang, Sterling Williams-Ceci, Sanketh Menda, and Amy X Zhang. 2023. " Is Reporting Worth the Sacrifice of Revealing What I Have Sent?": Privacy Considerations When Reporting on End-to-End Encrypted Platforms. *arXiv preprint arXiv:2306.10478* (2023).
[117] Rick Wash and Molly M Cooper. 2018. Who provides phishing training? facts, stories, and people like me. In *Proceedings of the 2018 chi conference on human factors in computing systems*. 1–12.
[118] Rick Wash, Norbert Nthala, and Emilee Rader. 2021. Knowledge and capabilities that {Non-Expert} users bring to phishing detection. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*. 377–396.
[119] Dominik Wermke, Nicolas Huaman, Christian Stransky, Niklas Busch, Yasemin Acar, and Sascha Fahl. 2020. Cloudy with a chance of misconceptions: exploring users' perceptions and expectations of security and privacy in cloud office suites. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. 359–377.
[120] Fiona Westin and Sonia Chiasson. 2021. "It's So Difficult to Sever that Connection": The Role of FoMO in Users' Reluctant Privacy Behaviours. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–15.
[121] Alma Whitten and J Doug Tygar. 1999. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0.. In *USENIX security symposium*, Vol. 348. 169–184.
[122] Daricia Wilkinson, Paritosh Bahirat, Moses Namara, Jing Lyu, Arwa Alsubhi, Jessica Qiu, Pamela Wisniewski, and Bart P Knijnenburg. 2020. Privacy at a glance: the user-centric design of glanceable data exposure visualizations. (2020).
[123] Aneka Williams, Grace Fox, Mary Jean Amon, Tangila Islam Tanni, and Yan Solihin. 2025. The GenAI networked privacy problem at work-How privacy knowledge and perceptions predict Generative AI disclosure in professional contexts. In *Proceedings of the Extended Abstracts of the CHI Conference on Human Factors in Computing Systems*. 1–9.
[124] Xiaodong Wu, Ran Duan, and Jianbing Ni. 2024. Unveiling security, privacy, and ethical concerns of ChatGPT. *Journal of information and intelligence* 2, 2 (2024), 102–115.
[125] Yuxi Wu, Panya Gupta, Miranda Wei, Yasemin Acar, Sascha Fahl, and Blase Ur. 2018. Your secrets are safe: How browsers' explanations impact misconceptions about private browsing mode. In *Proceedings of the 2018 World Wide Web Conference*. 217–226.
[126] Madelyne Xiao, Mona Wang, Anunay Kulshrestha, and Jonathan Mayer. 2023. Account Verification on Social Media: User Perceptions and Paid Enrollment. *arXiv preprint arXiv:2304.14939* (2023).
[127] Yucheng Yang, Jack West, George K Thiruvathukal, Neil Klingensmith, and Kassem Fawaz. 2022. Are you really muted?: A privacy analysis of mute buttons in video conferencing apps. *arXiv preprint arXiv:2204.06128* (2022).
[128] Seounmi Youn. 2005. Teenagers' perceptions of online privacy and coping behaviors: a risk–benefit appraisal approach. *Journal of Broadcasting & Electronic Media* 49, 1 (2005), 86–110.
[129] Shikun Zhang, Yuanyuan Feng, Lujo Bauer, Lorrie Faith Cranor, Anupam Das, and Norman Sadeh. 2021. "Did you know this camera tracks your mood?": Understanding Privacy Expectations and Preferences in the Age of Video Analytics. *Proceedings on Privacy Enhancing Technologies* 2021, 2 (2021).
[130] Jun Zhao, Ge Wang, Carys Dally, Petr Slovak, Julian Edbrooke-Childs, Max Van Kleek, and Nigel Shadbolt. 2019. I make up a silly name' Understanding Children's Perception of Privacy Risks Online. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–13.
[131] Sarah Zheng and Ingolf Becker. 2022. Presenting Suspicious Details in {User-Facing} E-mail Headers Does Not Improve Phishing Detection. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*. 253–271.
[132] Sebastian Zimmeck, Oliver Wang, Kuba Alicki, Jocelyn Wang, and Sophie Eng. 2023. Usability and enforceability of global privacy control. *Proceedings on Privacy Enhancing Technologies* 2 (2023), 1–17.
[133] Noé Zufferey, Kavous Salehzadeh Niksirat, Mathias Humbert, and Kévin Huguenin. 2023. "Revoked just now!" Users' Behaviors toward Fitness-Data Sharing with Third-Party Applications. *Proceedings on Privacy Enhancing Technologies* 2023, 1 (2023), 21.

9 ABOUT THE AUTHORS

- **Reza Shahriari** is a Ph.D. candidate with the University of Florida and the primary contact of this paper. His research interests include human–computer interaction, human-centered AI/XAI, and information visualization. He is the corresponding author of this article.

- **Eric D. Ragan** is an associate professor with the University of Florida. His research interests include human–computer interaction, visual analytics, virtual reality, and XAI systems.