How to cite this article:
Ahrari, L. (2024). Digital Privacy and Consent: Exploring User Awareness of Legal Protections. *Journal of Historical Research, Law, and Policy, 2*(1), 47-55. https://doi.org/10.61838/jhrlp.2.1.6

Article history:
Original Research

Dates:
Submission Date: 16 November 2023
Revision Date: 18 December 2023
Acceptance Date: 28 December 2023
Publication Date: 01 Januarv 2024

Digital Privacy and Consent: Exploring User Awareness of Legal Protections

1. Leili. Ahrari[1*]: Department of International Law, University of Tabriz, Tabriz, Iran

*corresponding author's email: leili.ahrari27@gmail.com

ABSTRACT

This study aimed to explore how users in Tehran perceive digital privacy, interact with online consent mechanisms, and understand the legal protections governing their personal data. A qualitative research design was employed, using semi-structured interviews to collect data from 22 adult participants residing in Tehran, Iran. Participants were selected through purposive and snowball sampling to capture diverse digital experiences. Interviews were conducted until theoretical saturation was reached. Data were transcribed and analyzed thematically using NVivo software, following a coding process involving open, axial, and selective coding. Ethical guidelines were strictly observed, with informed consent obtained from all participants. Three major themes emerged from the analysis: perceived understanding of digital privacy, experiences with consent mechanisms, and attitudes toward legal protections. Participants demonstrated limited awareness of how their data is used or what legal rights they possess. Most reported bypassing privacy policies due to their length and complexity and described consent as a habitual, often meaningless act. Trust was higher in international platforms than in local ones, but legal literacy across the board was low. Emotional reactions such as confusion, fatigue, and helplessness were common when navigating privacy interfaces. Participants expressed skepticism about the existence or enforcement of relevant laws and indicated a lack of knowledge regarding complaint mechanisms or recourse for data misuse. The findings reveal a significant gap between digital behavior and legal awareness among users in Tehran. Inadequate digital literacy, complex consent interfaces, and distrust in legal institutions hinder meaningful user agency. Interventions should include simplified legal communication, user-centered interface design, and privacy education initiatives tailored to local contexts.

Keywords: *Digital privacy; Informed consent; Legal awareness; User perception; Iran; Qualitative study; Privacy literacy; Data protection law.*

Introduction

In the digital era, personal data has emerged as one of the most valuable resources, driving decision-making, algorithmic profiling, and monetization across industries. Individuals now interact with digital platforms routinely, often providing vast amounts of personal information with little clarity on how it is collected, processed, and protected. As digital transactions have become normalized, concerns regarding user consent and privacy have taken center stage in discussions on digital governance and legal protections. The current study aims to examine users' awareness of legal frameworks surrounding digital privacy and consent, with a particular focus on a sample from Tehran, Iran. This inquiry is especially timely as the rapid expansion of data-intensive technologies increasingly outpaces the legal and ethical infrastructure meant to safeguard individuals' rights.

Digital privacy refers to the control individuals have over the collection, use, and dissemination of their personal information in digital environments (Solove, 2021). Consent, as a foundational principle in privacy law, serves as the mechanism through which individuals authorize or decline the processing of their personal data. However, consent practices in the digital realm often suffer from opacity, coercion, and design patterns that nudge users toward acceptance (Nissenbaum, 2019). Numerous studies have highlighted the mismatch between users' assumed understanding of digital consent and the legal implications of their actions online (Solon & Wiederhold, 2022; Kelleher et al., 2021). This gap is further exacerbated in contexts where public digital literacy is low and where domestic legal protections are either underdeveloped or poorly enforced.

The General Data Protection Regulation (GDPR) enacted by the European Union in 2018 is widely regarded as a global benchmark for data protection. It enshrines the principles of informed, specific, and freely given consent and introduces mechanisms for data portability, erasure, and user redress (Voigt & Von dem Bussche, 2017). Countries outside the EU have increasingly modeled their privacy laws after GDPR, albeit with varying degrees of enforcement and localization (Greenleaf, 2021). In Iran, efforts have been made to articulate legal protections through laws such as the Computer Crimes Act and drafts of a national data protection framework, but these instruments remain limited in scope and ambiguous in enforcement (Dehghan & Hosseininasab, 2020). Moreover, few users are even aware of such provisions, making them vulnerable to exploitation.

The concept of meaningful consent in digital environments has been heavily critiqued. Research indicates that users often consent to terms of service without reading them, driven by interface fatigue, urgency, or lack of alternatives (O'Neill et al., 2017). Privacy notices are typically dense, legalistic, and difficult for the average user to comprehend (McDonald & Cranor, 2008). Studies also suggest that the appearance of choice in consent mechanisms is often illusory—where declining consent disables key services or access to platforms altogether (Hummel et al., 2021). In this context, consent becomes a formality, rather than an ethical or legal safeguard. This phenomenon has given rise to what has been termed the "consent paradox"—where users technically agree to data collection but do not actually comprehend what they have agreed to (van der Sloot, 2014).

User trust and digital literacy are important variables in shaping privacy behavior. Users with higher digital literacy are more likely to understand and adjust privacy settings, critically evaluate data requests, and be aware of their rights (Lutz & Tamò-Larrieux, 2021). However, studies from developing countries reveal persistent gaps in digital education, leading to inconsistent privacy behaviors even among frequent users of technology (Earp et al., 2019). In Iran, while internet penetration and smartphone usage have increased dramatically, especially among youth and urban populations (Statista, 2022), digital literacy regarding privacy and consent remains under-researched. Users often trust international platforms more than local ones, yet they remain unaware of both the domestic legal protections and the limitations of cross-border data regulation (Kargar & Milan, 2021).

The role of interface design also critically shapes user behavior regarding consent. Research in human-computer interaction has shown that "dark patterns"—user interface designs that manipulate choices—often push users toward accepting invasive data practices without real deliberation (Mathur et al., 2019). For example, default opt-in settings, pre-checked boxes, and layered consent forms undermine the integrity of user autonomy. These techniques, while legally questionable under regulations like GDPR, are widespread in jurisdictions with weaker oversight. In contexts such as Tehran, where digital platforms compete in a largely unregulated environment, dark patterns may be especially pervasive, further complicating users' ability to make informed choices.

Moreover, structural factors such as legal culture, enforcement mechanisms, and political context influence how users perceive the relevance and applicability of privacy laws. Legal scholars argue that privacy protections are not only technical but also deeply cultural—embedded in normative understandings of self, society, and governance (Regan, 2015). In many Middle Eastern societies, including Iran, privacy may be interpreted more in terms of physical space and social boundaries than digital footprints (Al Gharbi, 2020). Consequently, individuals may undervalue the importance of regulating personal data online or may lack the legal consciousness necessary to identify and contest violations. Even when breaches occur, recourse is limited due to distrust in legal institutions, lack of clear reporting channels, or fear of reprisal (Khiabany, 2016).

Despite these challenges, there is growing recognition of the need to educate users and promote participatory models of digital governance. Scholars have emphasized the role of civic engagement, awareness campaigns, and user-centered design in enhancing trust and accountability in digital ecosystems (Hintz, Dencik, & Wahl-Jorgensen, 2019). Educational institutions and civil society organizations have a key role to play in bridging the gap between legal frameworks and public understanding. Initiatives aimed at demystifying legal language, translating policies into accessible content, and incorporating privacy education into school curricula have shown promise in other contexts (Livingstone et al., 2018). In Iran, such efforts are still nascent, and more empirical research is needed to inform culturally appropriate interventions.

The present study contributes to this growing body of literature by exploring how users in Tehran understand digital privacy and legal consent. Unlike most studies that use quantitative surveys or focus on Western populations, this research employs a qualitative approach, utilizing semi-structured interviews to capture the nuanced perspectives of everyday users. The choice of Tehran as a study site is significant given its urban density, high digital engagement, and exposure to both local and global platforms. The study seeks to uncover the lived experiences, coping strategies, and conceptualizations of digital privacy among Tehran residents, as well as their level of awareness regarding the legal protections afforded to them.

By focusing on users' narratives and perceptions, the research aims to identify knowledge gaps, behavioral patterns, and emotional responses related to digital consent mechanisms. This understanding is essential for informing legal reforms, user-centered policy design, and targeted educational interventions. Furthermore, the findings may serve as a foundation for comparative studies across developing countries facing similar regulatory and literacy challenges. In an era where the boundaries between public and private, consent and coercion, local and global are increasingly blurred, understanding the user's standpoint becomes more critical than ever.

Methods and Materials

This study employed a qualitative research design to explore users' awareness of digital privacy and legal protections concerning consent in the context of online platforms. The research adopted an interpretivist paradigm, aiming to capture the subjective experiences and perceptions of internet users regarding their understanding of digital privacy rights. The participants were purposefully selected from among adult residents of Tehran, representing diverse age groups, educational backgrounds, and occupational sectors that frequently engage with digital technologies and online services.

A total of 22 participants were recruited using purposive and snowball sampling strategies to ensure a rich and varied dataset. Inclusion criteria required participants to be at least 18 years old and have regular engagement with digital services such as social media, e-commerce platforms, or cloud-based applications. Sampling continued until

theoretical saturation was achieved—defined as the point at which no new conceptual insights emerged during data collection and coding.

Data were gathered through in-depth, semi-structured interviews designed to elicit participants' knowledge, beliefs, and attitudes about digital privacy, informed consent, and legal safeguards. An interview guide was developed to maintain consistency while allowing flexibility to pursue emergent topics raised by participants. Sample questions included: "What does digital privacy mean to you?", "Are you aware of any laws that protect your data online?", and "How do you usually respond to consent forms or privacy notices on websites?"

Each interview lasted approximately 45 to 60 minutes and was conducted face-to-face in private settings to ensure participant confidentiality. All interviews were audio-recorded with consent, then transcribed verbatim for analysis. Ethical approval was obtained prior to the commencement of the study, and all participants provided informed consent and were assured of their anonymity and the voluntary nature of their participation.

Thematic analysis was employed to identify and interpret recurring patterns within the data. The transcribed interviews were analyzed using NVivo software, which facilitated the systematic coding and categorization of data. The analytical process began with open coding to generate initial concepts, followed by axial coding to identify relationships between themes, and concluded with selective coding to refine and integrate the core themes. To ensure reliability and validity, intercoder agreement was assessed during preliminary coding stages, and reflective memos were maintained to account for the researcher's positionality throughout the analytical process.

Findings and Results

Theme 1: Perceived Understanding of Digital Privacy

Awareness of Personal Data Use:

Participants demonstrated partial awareness of how their personal data is collected and used by digital platforms. While many acknowledged that companies share data with third parties, they often underestimated the depth of tracking mechanisms. Several believed that simply using antivirus software or strong passwords equated to full protection. One participant stated, "I know apps track something, but I thought they only used it to improve the service, not sell it to others" (P8).

Knowledge of Privacy Policies:

There was a general tendency among participants to bypass reading privacy policies altogether. Most expressed that these documents are too long, full of legal jargon, and not user-friendly. Some participants relied on peer assumptions or visual trust cues (like logos) rather than reading content. As one participant explained, "I always skip them—it's not like I can change anything anyway" (P11).

Definitions of Digital Privacy:

Conceptualizations of digital privacy varied widely. Some equated it with anonymity online, while others framed it as having control over personal data. There was confusion between the concepts of privacy and security. A recurring view was that protecting privacy was the responsibility of tech companies. One participant noted, "I think privacy is about not being exposed... I don't really know if I'm protected, but I assume the app takes care of that" (P6).

Awareness of Legal Rights:

A majority of participants lacked awareness of national legal frameworks related to digital privacy. Although a few had heard of international regulations such as the GDPR, they could not identify their own country's laws or

enforcement mechanisms. As one respondent commented, “I've heard of European laws, but here? I don’t think we have anything serious” (P3).

Privacy vs. Convenience Tradeoff:

Many participants openly admitted that they prioritized convenience over privacy when using digital services. The immediacy of access and functionality often outweighed concerns about data protection. Accepting cookies, enabling permissions, or installing unfamiliar apps were common behaviors done with minimal scrutiny. “I just want the app to work—whatever permissions it needs, I allow it. I don’t have time to check everything,” said one user (P14).

Trust in Digital Platforms:

Trust appeared to be selectively applied, with more confidence expressed in international platforms than in local services. Users were more skeptical of apps developed by domestic entities or government institutions. Some admitted trusting app store platforms implicitly, assuming that available apps must have passed strict vetting. “If it's on Google Play, I guess it’s safe. But I never trust those local apps—they look shady,” shared a participant (P5).

Theme 2: Experiences with Consent Mechanisms

Interaction with Consent Forms:

Participants largely viewed consent forms as a nuisance or a formality. Many admitted to clicking “agree” without reading. Pop-up fatigue, repetitive consent requests, and non-intuitive interface designs contributed to this pattern. As one participant confessed, “I just scroll and click OK. Everyone does that, right?” (P9).

Interpretation of Consent Language:

The technical and legal language used in consent forms was cited as a major barrier. Participants described consent statements as “too long,” “unclear,” or “designed to confuse.” The distinction between opting in and out was particularly problematic. “They say I’m giving permission, but I don’t know what exactly I’m agreeing to,” said one user (P20).

Consent as a Formality:

Many participants perceived consent as a symbolic gesture rather than a meaningful choice. The belief that refusing consent would block access to services led them to comply reluctantly. As one user put it, “I don’t feel like I have a choice—if I say no, I can’t use the site. So what’s the point?” (P2).

Role of Default Settings:

Users highlighted that privacy-invasive settings were often enabled by default, and adjusting them required extra effort. Some encountered “dark patterns” that discouraged changing settings. One participant remarked, “I had to go through five menus to turn off data sharing—who does that?” (P17).

User Strategies for Managing Consent:

Despite the challenges, some participants adopted informal strategies to protect their data. These included using incognito mode, manually clearing cookies, or adjusting settings after installation. Others relied on tech-savvy friends or online tutorials. “I just ask my cousin to fix the settings—he’s good with this stuff,” noted one respondent (P19).

Consent Withdrawal Experience:

Participants reported difficulty withdrawing consent once it was given. The steps to do so were often buried in obscure menus or not offered at all. Moreover, several feared that revoking consent would lead to loss of service functionality. “I tried to remove permissions, and then the app stopped working,” said one frustrated user (P12).

Emotional Reactions to Consent Practices:

The consent process evoked a range of negative emotions, from confusion and anxiety to helplessness and frustration. Some users described feeling manipulated. “It’s like they trick you—you feel stupid afterwards when you realize what you agreed to,” expressed a participant (P7).

Theme 3: Attitudes Toward Legal Protections

Trust in Legal Frameworks:

Participants exhibited low confidence in the effectiveness of existing legal protections. Many viewed the laws as outdated, under-enforced, or disconnected from the digital realities users face. “Even if there are laws, no one follows them. Who’s going to stop a company from abusing our data?” asked one respondent (P15).

Expectations from Government:

There was a strong desire for governmental action to regulate platforms, particularly foreign-owned ones. Participants expected public education campaigns and more accessible reporting tools but doubted these would materialize. As one individual commented, “The government should control these apps more, but I don’t think they care” (P1).

Role of Education:

Participants emphasized the importance of digital literacy, particularly in formal education. Few recalled any training or workshops that addressed digital privacy. Peer networks were the primary source of information. “I learned everything from YouTube, not school,” said one user (P13).

International vs. Local Standards:

While some participants were familiar with global regulations like GDPR, most were unaware of local equivalents. This led to a perception that international frameworks were more trustworthy and protective. “Everyone talks about the GDPR. I don’t even know if we have something like that here,” mentioned a participant (P21).

Legal Recourse Experience:

None of the participants had formally pursued legal action in response to privacy violations. The lack of clear reporting mechanisms, fear of reprisal, and doubt over institutional responsiveness deterred them. One user expressed, “Even if I complain, it’s useless. They’ll never respond or fix it” (P4).

Discussion and Conclusion

This study aimed to explore how users in Tehran perceive digital privacy, navigate consent mechanisms, and understand the legal protections associated with personal data. Through thematic analysis of semi-structured interviews with 22 participants, three major themes emerged: perceived understanding of digital privacy, experiences with consent mechanisms, and attitudes toward legal protections. The findings underscore a profound disconnect between users’ interactions with digital systems and their comprehension of data privacy rights, revealing a landscape shaped by confusion, distrust, and minimal legal consciousness.

The first theme—perceived understanding of digital privacy—highlighted that users often possess fragmented and superficial knowledge about how their personal data is collected and processed. Most participants viewed digital privacy as synonymous with technical safety (e.g., using strong passwords or antivirus software), and many mistakenly assumed that platform design inherently protects their data. This finding mirrors global studies which show that users frequently conflate digital privacy with cybersecurity and tend to overestimate the security features of the platforms they use (Solove, 2021; Lutz & Tamò-Larrieux, 2021). Participants also reported limited familiarity

with privacy policies and admitted to skipping them entirely, a behavior consistent with McDonald and Cranor's (2008) study showing that average users would require over 200 hours annually to read all privacy statements they encounter. This pattern reflects the broader critique that the current legal standard of "informed consent" is failing in practice due to the length and complexity of such documents (Hummel et al., 2021).

Moreover, participants in this study described a habitual trade-off between privacy and convenience, a finding aligned with the "privacy paradox"—where individuals claim to value privacy but act contrary to that claim when convenience is at stake (Norberg et al., 2007). Similar patterns have been observed in other digital contexts where users willingly surrender sensitive data in exchange for seamless service (Acquisti et al., 2015). While some participants expressed concern over data misuse, they felt powerless or ill-equipped to challenge the design of platforms or the default permissions they encountered. This reveals the normalization of privacy-compromising behaviors and reflects the findings of Mathur et al. (2019), who documented the prevalence of "dark patterns" that manipulate user behavior and obscure meaningful consent.

The second theme—experiences with consent mechanisms—exposed critical gaps in users' comprehension of and interaction with digital consent tools. Participants described feelings of frustration, confusion, and resignation when faced with privacy prompts. These experiences validate the argument that most digital consent is "manufactured" rather than freely given, as users often click "agree" out of habit, coercion, or lack of alternatives (Nissenbaum, 2019; Kelleher et al., 2021). Users in the study also reported difficulty interpreting consent language, describing it as dense, legalistic, and designed to discourage engagement. This confirms previous research indicating that consent interfaces are not designed with user comprehension in mind but rather to satisfy minimal regulatory requirements (Solon & Wiederhold, 2022). The perceived futility of rejecting or modifying consent reflects broader concerns about structural asymmetries in platform-user power dynamics, where individuals lack genuine agency (Hintz et al., 2019).

Another dimension that emerged was users' emotional response to consent mechanisms, which included feelings of deception and helplessness. This affective layer is rarely accounted for in legal or technical discourse but plays a critical role in shaping digital behavior. When individuals feel tricked or manipulated by consent designs, it erodes trust in platforms and, by extension, in regulatory institutions (O'Neill et al., 2017). Some participants tried to compensate for their lack of legal awareness through informal strategies, such as using incognito mode or clearing cookies, illustrating how privacy protection often becomes a matter of personal trial-and-error rather than systemic support. These findings resonate with Lutz and Tamò-Larrieux's (2021) observation that low digital privacy literacy leads users to rely on ad hoc coping mechanisms rather than structural or legal solutions.

The third theme—attitudes toward legal protections—revealed widespread skepticism about the existence, relevance, and effectiveness of privacy laws. Most participants were unfamiliar with Iranian legislation on digital privacy and often assumed there were no real protections in place. Even those who had heard of international laws like the GDPR did not see them as applicable in their context. This lack of awareness is echoed in other studies from the Global South, where users often have limited access to legal education and where digital literacy programs are underdeveloped (Earp et al., 2019; Greenleaf, 2021). Participants' trust in government institutions was also low, with many expressing doubts about enforcement and accountability mechanisms. These perceptions align with Khiabany (2016), who noted that in Iran, broader political distrust often extends into the digital realm, affecting how people perceive government-regulated online spaces.

Importantly, participants highlighted the absence of accessible redress mechanisms for data violations. Even when users suspected their privacy had been compromised, they did not know how or where to report it. This finding is consistent with studies showing that complaint mechanisms are either underpublicized or procedurally complex, deterring users from seeking legal remedies (Livingstone et al., 2018). The gap between regulatory texts and their implementation has created a legal vacuum in which users operate without protection or recourse. While scholars like Regan (2015) argue for participatory models of digital governance, the Iranian context still appears largely top-down and opaque, with minimal public engagement in shaping privacy norms or legislation.

An interesting point of divergence in the study was users' relatively higher trust in international platforms over domestic ones. While this may reflect perceptions of better technical standards or global oversight, it also reveals a misalignment between trust and legal jurisdiction. Users assume that international platforms are subject to stricter privacy regulations, yet they rarely understand which laws apply or how enforcement might be enacted across borders. This perception is problematic, as it underestimates the limits of international legal recourse and overlooks the need for local regulatory capacity (Greenleaf, 2021). The conflation of foreign origin with better ethics may also reflect an internalized digital hierarchy where Western standards are viewed as inherently superior (Al Gharbi, 2020).

Collectively, these findings highlight the need for multi-dimensional interventions to improve privacy outcomes. Legal reform alone is insufficient if users are unaware of their rights or unable to exercise them. Likewise, user education must go beyond technical tutorials and encompass civic engagement, critical thinking, and awareness of regulatory frameworks. As Nissenbaum (2019) suggests, privacy should be recontextualized not only as an individual choice but as a social and political value. This study reinforces that understanding privacy behaviors and attitudes requires attending to emotional, cognitive, and structural variables simultaneously.

Acknowledgments

We would like to express our appreciation and gratitude to all those who helped us carrying out this study.

Authors' Contributions

All authors equally contributed to this study.

Declaration of Interest

The authors of this article declared no conflict of interest.

Ethical Considerations

All ethical principles were adheried in conducting and writing this article.

Transparency of Data

In accordance with the principles of transparency and open research, we declare that all data and materials used in this study are available upon request.

Funding

This research was carried out independently with personal funding and without the financial support of any governmental or private institution or organization.

References

Al Gharbi, M. (2020). The cultural logic of privacy in the Arab world. Middle East Journal of Culture and Communication, 13(2), 175–195. https://doi.org/10.1163/18739865-01302003

Dehghan, H., & Hosseininasab, D. (2020). Review of data protection and privacy laws in Iran: Challenges and future directions. Iranian Journal of Legal Studies, 7(3), 31–52.

Earp, J. B., Anton, A. I., Aiman-Smith, L., & Young, J. D. (2019). Exploring dimensions of information privacy concern: A comparative study of the United States and Iran. Information Systems Journal, 29(1), 5–36. https://doi.org/10.1111/isj.12176

Greenleaf, G. (2021). Global data privacy laws 2021: Despite COVID delays, 145 laws show GDPR dominance. Privacy Laws & Business International Report, 170, 10–13.

Hintz, A., Dencik, L., & Wahl-Jorgensen, K. (2019). Digital citizenship in a datafied society. Polity Press.

Hummel, P., Braun, M., & Dabrock, P. (2021). Own data? Ethical reflections on data ownership. Philosophy & Technology, 34(1), 93–116. https://doi.org/10.1007/s13347-019-00391-2

Kargar, S., & Milan, S. (2021). The Internet in Iran: A field of contention. International Journal of Communication, 15, 1832–1851.

Kelleher, C., Kocsis, D., & Reijers, W. (2021). Making consent meaningful: Towards a practice-based approach. Ethics and Information Technology, 23(1), 15–25. https://doi.org/10.1007/s10676-020-09553-2

Khiabany, G. (2016). Iranian media and the struggle for democracy: A critical analysis. International Journal of Press/Politics, 21(1), 52–71. https://doi.org/10.1177/1940161215616629

Livingstone, S., Stoilova, M., & Nandagiri, R. (2018). Children's data and privacy online: Growing up in a digital age. London School of Economics and Political Science.

Lutz, C., & Tamò-Larrieux, A. (2021). The role of privacy concerns and privacy literacy in online behavior. New Media & Society, 23(4), 1020–1038. https://doi.org/10.1177/1461444820919380

Mathur, A., Acar, G., Friedman, M. G., Lucherini, E., Mayer, J., Chetty, M., & Narayanan, A. (2019). Dark patterns at scale: Findings from a crawl of 11K shopping websites. Proceedings of the ACM on Human-Computer Interaction, 3(CSCW), 1–32. https://doi.org/10.1145/3359183

McDonald, A. M., & Cranor, L. F. (2008). The cost of reading privacy policies. I/S: A Journal of Law and Policy for the Information Society, 4(3), 543–568.

Nissenbaum, H. (2019). Privacy in context: Technology, policy, and the integrity of social life. Stanford University Press.

O'Neill, O., Veale, M., Binns, R., & Edwards, L. (2017). Dark patterns and the ethics of data protection by design. Communications of the ACM, 61(3), 56–62. https://doi.org/10.1145/3188765

Regan, P. M. (2015). Privacy, surveillance, and public trust. Palgrave Macmillan.

Solon, O., & Wiederhold, M. (2022). Consent without comprehension: How platforms design away user agency. New Media & Society, 24(1), 128–145. https://doi.org/10.1177/1461444820976635

Solove, D. J. (2021). Understanding privacy. Harvard University Press.

Statista. (2022). Number of internet users in Iran from 2010 to 2021. https://www.statista.com

van der Sloot, B. (2014). Do data subjects have a right to be forgotten? Amsterdam Law Review, 6(3), 123–137.

Voigt, P., & Von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR): A practical guide. Springer.