Drivers and Passengers May be the Weakest Link in the CAV Data Privacy Defenses

Aiping Xiong
Pennsylvania State University
axx29@psu.edu

Zekun Cai
Pennsylvania State University
zuc204@psu.edu

Tianhao Wang
University of Virginia
tianhao@virginia.edu

***Abstract*—Individuals' interactions with connected autonomous vehicles (CAVs) involve sharing various data in a ubiquitous manner, raising novel challenges for privacy. The *human factors* of privacy must first be understood to promote consumers' acceptance of CAVs. To inform the privacy research in the context of CAVs, we discuss how the emerging technologies development of CAV poses new privacy challenges for drivers and passengers. We argue that the privacy design of CAVs should adopt a user-centered approach, which integrates human factors into the development and deployment of privacy-enhancing technologies, such as differential privacy.**

I. Introduction

While the data collection and analysis capabilities of connected autonomous vehicles (CAVs) are under rapid development, drivers' and other occupants' disclosure behaviors must first be investigated to improve the acceptance and facilitate the development of CAVs [59]. The massive amounts of heterogeneous data (e.g., driving and vehicle data, trip data, and drivers' and passengers' personal information) collected and used by the CAVs raise novel challenges for users' adequate privacy awareness and informed privacy decisions.

People regulate their privacy through dynamic processes of awareness, decision making, and action selection [4]. Privacy concerns refer to people's privacy-related attitudes [34], which are shaped by users' awareness of privacy-relevant information [53], [56]. Nevertheless, people are typically ill-informed of the nature and purpose of data collection, as well as the associated costs, benefits, and risks [8]. Moreover, privacy concerns are usually measured in the contexts of disclosure requests instead of *how* the data are being used (e.g., surveillance and digital tracking). Privacy awareness is a prerequisite to making informed decisions. Yet, increased privacy awareness does not necessarily ensure more conservative privacy decisions [3], [46].

Individuals' online disclosure choices are context-dependent [38] and contingent on their mental capacity [58]. Prior literature has shown that people's privacy decision-making is affected and sometimes impaired by *biased* human information processing [1], [2], [58]. Previous studies have also revealed a gap between individuals' stated disclosure intentions and actual data-sharing behaviors [8], [23], [40], called the *privacy paradox*.

While considerable studies have been conducted to address the privacy of CAVs from the technical perspective [17], [24], [44], few studies investigated the privacy issues from the human factors' perspective [9], [11]. Similar to other well-studied systems such as mobile phones or the Internet of Things (IoT), those prior works have mainly shown that users' have privacy concerns about data sharing [11] and use [9] of CAVs. However, the uniqueness of the CAV privacy has not been systematically evaluated from the users' perspective.

In this preliminary work, we seek to understand the human factors in the privacy of CAVs. We review factors that affect different privacy-related behaviors (e.g., privacy awareness, privacy decision-making, and privacy action selection) and discuss novel challenges imposed by the unique CAVs contexts. We then discuss the role of human factors in deploying privacy-enhancing technologies (e.g., differential privacy) in the CAV contexts.

II. Privacy Contexts for CAVs

An investigation on the potential interactions between privacy and CAVs is very challenging since CAVs are under development [51] and the concept of privacy is complex and difficult to define [39]. The operation of CAVs relies on their sensors' data. Recently, for better road operation and safety, intelligent traffic system (ITS) has been proposed, which will provide transport networks, operations, and services for CAVs [31], [42]. Meanwhile, Vehicle-to-Everything (V2X) communication has also been proposed, in which information from on-board sensors and other sources travels via high-bandwidth wireless links, such as communication with other vehicles (V2V) and with the road infrastructure (V2I) [18].

Instead of ascribing privacy as fixed and static, the subjective importance of privacy can change over time, across contexts, and as a result of external factors [38]. Considering the difficulty of managing *who* collects *what* kinds of data in the ubiquitous data collection along with driving, we focus on the question of *how* the data are being used, that is, in which context and for which purpose, for the privacy of CAVs. Generally, ITS applications can be separated into the four categories: 1) autonomous driving, 2) road safety, 3) traffic management, and 4) infotainment and comfort [17].

Workshop on Automotive and Autonomous Vehicle Security (AutoSec) 2022
24 April 2022, San Diego, CA, USA
ISBN 1-891562-75-4
https://dx.doi.org/10.14722/autosec.2022.23024
www.ndss-symposium.org

a) Autonomous Driving: Self-driving applications mainly rely on sensors inside and outside the vehicles (e.g., LiDAR and RADAR) to achieve automobile recognition as well as other driving functions. For example, ultrasonic sensors are used to detect obstructions (e.g., humans or animals) for automatic braking.

b) Road Safety: V2X communication is the main application used to enhance road safety (i.e., the safety of drivers, passengers, and people on the road), including V2V (vehicle to vehicle), V2I (vehicle to infrastructure) and V2P (vehicle to pedestrians). Besides vehicle speed control, accidents, alerts, and emergencies on the road (e.g., collision warning) can be communicated through enabling the communication of signals and messages of all interconnected entities in ITS.

c) Traffic Management: Data collection and use in the traffic management applications are to provide detailed information concerning cars, drivers, and status on the roads, which are expected to enhance traffic flow control and synchronization and provide drivers with cooperative traffic services. For example, these applications will collect and analyze the messages exchanged by ITS entities and communicate to CAV users of existing congested zones. Traffic data (e.g., a pedestrian is crossing the road) can also be obtained by the deployed roadside units (RSUs) and the road sensors to prevent accidents from occurring.

d) Infotainment and Comfort: Data collection and use in these applications aim to enhance user experience in the driving cockpit through services that meet their needs. For example, connectivity to the Internet is expected to be offered to provide access to services, such as online music and videos. Such applications are close to the applications in most mobile devices, which also include weather services, navigation, and entertainment.

How the data are being used in CAVs can be presented in more granular levels (e.g., entities such as RSUs and onboard units within ITS). Yet, the above coarse-level categorization is useful to help us identify major, novel challenges, which we discuss in the next section.

III. Human Factors in the Privacy of CAVs

Using the human information-processing approach [61], we characterize that individuals process privacy via stages of *privacy motivation*, *privacy awareness*, *privacy decisions*, and *privacy actions*. For each stage, we first introduce human factors that have been identified influencing the privacy in the general online environment [50], [57]. We then discuss the uniqueness of each stage in the CAV contexts.

a) Privacy Motivation: Individuals are motivated to share information online by various goals, such as economic benefits [30], psychological benefits and social benefits [12]. While the effects of those disclosure decisions (e.g., lower price, psychological pleasure, and social engagements) are typically immediate or in a relatively short term, possible information leakage or privacy risks are typically delayed or occur in the future. When comparing benefits in exchange for personal information and protection of their personal information but at some cost (i.e., privacy utility tradeoff), people often choose immediate, smaller gains over delayed, larger gains (i.e., delay discounting) [28], [29], resulting in more willingness to share information under the disclosure request.

Compared to the general online environment, individuals have novel motives to share personal information in different CAV contexts. Specifically, *driving safety* could become individuals' primary motives for data disclosure (e.g., concerns about fatal CAV accidents due to not sharing some data). While the safety issues might be distal, people probably choose to share the data anyway due to the severe consequences of not sharing. Therefore, the existing privacy-utility tradeoff becomes privacy-utility and privacy-safety tradeoffs in the CAV contexts (Fig 1), which could make drivers and passengers become the even weaker link in the CAV data privacy defenses.

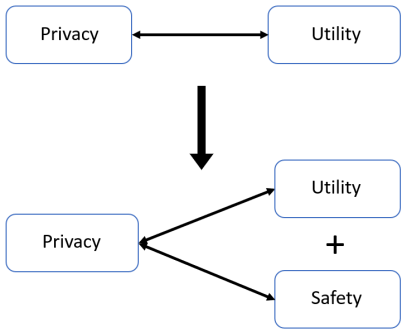

Fig. 1: Besides privacy-utility tradeoff, there is an extra privacy-safety tradeoff when users make disclosure decisions in various CAV contexts.

b) Privacy Awareness: Privacy awareness refers to people's attention and perception of possible risks throughout the interaction with an application or service that can gather and process personal data or information [46]. Individuals perceive (i.e., represent and understand) the environment through organizing, identifying, and interpreting sensory information (e.g., visual and auditory) [26]. Besides passively receiving information from the environment, human perception is often shaped by individuals' memory and expectations [27]. For example, people tend to pay more attention to information that is consistent with their prior knowledge or meets their expectations, resulting in disregarding some information (i.e., *incomplete information*) in decision making [10].

Online service providers generally adopt privacy policies to notify users of their data collection, dissemination, and use practices [45]. Nevertheless, those privacy policies are typically long [36] and not accessible to everyday users [22]. Online users rarely take time to read and understand the service providers' policies [6], [48]. Consequently, their awareness and comprehension of privacy-related information (e.g., diverse ways of collecting and processing online personal information) is likely to be low [49], resulting in *information asymmetry* between users and services providers [33].

V2X communication consists of information from on-board sensors and other sources traveling via high-bandwidth wireless links. V2X encompasses communication in three primary domains (i.e., V2V, V2I, and V2P). Numerous online services and data exchanges within each domain can have their own privacy policies. If adopting the implementation of current privacy policy, the information asymmetry of CAV users could be even more severe in the future.

Moreover, most communication of privacy to users is deployed using visual stimuli [52]. Since drivers' and passengers' visual attention is typically given to driving-related objects, auditory stimuli such as seat belt buckle alarms have been implemented to increase drivers' and passengers' awareness. Therefore, other *modalities* (e.g., auditory or tactile) signaling potential risks of data exchange inside or outside the driving cockpit might be expected by CAV users.

c) Privacy Decisions and Actions: Even if individuals can attend to all available information, their ability to translate the information into informed decisions is limited by *bounded rationality* [55]. In other words, individuals deviate the choices they make from the optimal choices assumed rational, revealing systematic biases. The privacy literature has identified various cognitive factors that affect and sometimes impede privacy decision-making [1]. We discuss heuristic decision-making that is closely relevant to the CAV contexts.

Given the information overloading and consequently incomplete information processing, individuals' privacy decision-making relies on the information first available to them (i.e., anchoring [14]), the information in the default privacy settings [7], how the information is framed (i.e., positively or negatively [15], [16], [47]), or the decisions of peers [13]. Even if individuals are not influenced by any of the above factors, the "dark" design intention that leverages human information-processing limitations [35], can also make the informed privacy decision-making becomes difficult.

Notice and consent have been implemented as the primary instrument for privacy decision-making and action selection [19], [52]. Recently, due to the GDPR, consent with more granular levels has been available for individuals to select with more options [41]. Nevertheless, providing more options may create a sense of control in data sharing, resulting in more data disclosure [2]. Online users can be overwhelmed by the number of choices that they have to select [43]. The proliferation of choice [54] reveals that more choices on disclosure decisions are not always better in a privacy context.

In the age of CAVs, notice and consent alone will be inadequate to protect individuals' privacy. As we have discussed above, the massive data exchange will feature privacy policies involving numerous parties, which raises unique challenges of effectively informing users of the frequently changing policies. Given the safety-sensitive nature of driving, any decision making or action selection in the driving cockpit may also be *time critical*. For example, the NHTSA guidelines have recommended that tasks to be completed by the driver while driving with glances away from the roadway of 2 seconds or less [32]. In case of any time-critical safety concerns, decisions and actions afforded by other modalities (e.g., voice control, gesture control, and steering wheel control), as well as solutions beyond notice and consent should also be considered in the CAV contexts. Moreover, data collection and sharing based on individual users' consent will have consequences affecting other users inside and outside the CAVs. For example, camera data shared by consented CAV drivers to facilitate traffic management might be used to profile non-consented pedestrians or other vehicles on the road.

IV. Privacy Enhancing Approaches

Privacy-enhancing technologies have been proposed to allow both data protection and data analytics in CAVs [5], including privacy based on perturbation using Differential Privacy (DP) [21]. DP has been emerged as the *de facto* standard for data privacy in academic and industry. In DP, the added random noise will protect the privacy of an individual user but reduce the utility of the aggregated-level data.

On the one hand, CAVs pose a higher demand for other privacy-enhancing technologies, such as secure multi-party computation [25] and federated data analytics [37]. One unique challenge is the real-time, large-volume data collection and sharing. Existing multi-party computation and federated data analytics are slow due to the requirements for privacy protection. To make these techniques more efficient, we need to use efficient processors, enable high network communication, and fine-tune in-vehicle operating system.

On the other hand, we should take a user-centered deployment [62] to ensure the success of those privacy-enhancing approaches in CAVs. Specifically, privacy-enhancing technologies (e.g., DP) should be informed by the human factors of privacy. For example, the privacy protection of DP comes at the cost of data accuracy. In the CAV contexts, users may have concerns about the negative influence on their safety and refuse to accept it. Thus, when deploying DP, it is important to be *transparent* on the utility cost, safety cost, and their implications. Given the heterogeneous data collected in the CAVs (e.g., driving and vehicle data, infotainment and comfort data), different DP trust models and different noise levels should be considered. For example, the privacy default could be set at a reasonable protection level and acceptable tradeoffs of privacy-utility and privacy-safety based on users' expectations. If users have concerns about the trustworthiness of the involving parties, local DP [20], [60] can be recommended. Moreover, the time-critical safety concerns must be considered when implementing DP in the CAV contexts. In other words, the implementation of DP should have minimal impacts on the safety-related performance of CAV users.

V. Conclusion

We advocate that privacy challenges from CAV drivers and passengers should be considered and proactively integrated into the development and deployment of privacy protection for CAVs. More frequent and better collaboration among industry leaders, computer scientists, and social scientists will be critical for usable privacy-enhancing technologies of CAVs.

ACKNOWLEDGEMENTS

This work was funded in part by a seed grant from Penn State's Center for Security Research and Education (CSRE).

REFERENCES

[1] A. Acquisti, L. Brandimarte, and G. Loewenstein, "Privacy and human behavior in the age of information," *Science*, vol. 347, no. 6221, pp. 509–514, 2015.

[2] ——, "Secrets and likes: the drive for privacy and the difficulty of achieving it in the digital age," *Journal of Consumer Psychology*, vol. 30, no. 4, pp. 736–758, 2020.

[3] A. Acquisti and J. Grossklags, "Privacy attitudes and privacy behavior," in *Economics of information security*. Springer, 2004, pp. 165–178.

[4] I. Altman, *The environment and social behavior: privacy, personal space, territory, and crowding*. Brooks/Cole Publishing Co., 1975.

[5] U. I. Atmaca, C. Maple, and M. Dianati, "Emerging privacy challenges and approaches in CAV systems," in *Proceedings of the 2019 Living in the Internet of Things: Cybersecurity of the IoT*, 2019, pp. 1–9.

[6] B. Auxier, L. Rainie, M. Anderson, A. Perrin, M. Kumar, and E. Turner, "Americans and privacy: Concerned, confused and feeling lack of control over their personal information," https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/, 2019.

[7] R. Balebako, P. G. Leon, H. Almuhimedi, P. G. Kelley, J. Mugan, A. Acquisti, L. Cranor, and N. Sadeh-Koniecpol, "Nudging users towards privacy on mobile devices," in *Proceedings of CHI-PINC*, 2011, pp. 1–4.

[8] S. Barth and M. D. De Jong, "The privacy paradox–investigating discrepancies between expressed privacy concerns and actual online behavior–a systematic literature review," *Telematics and Informatics*, vol. 34, no. 7, pp. 1038–1058, 2017.

[9] C. Bloom, J. Tan, J. Ramjohn, and L. Bauer, "Self-driving cars and data collection: Privacy perceptions of networked autonomous vehicles," in *Proceedings of Thirteenth Symposium on Usable Privacy and Security (SOUPS)*, 2017, pp. 357–375.

[10] T. Bolsen, J. N. Druckman, and F. L. Cook, "The influence of partisan motivated reasoning on public opinion," *Political Behavior*, vol. 36, no. 2, pp. 235–262, 2014.

[11] T. Brell, H. Biermann, R. Philipsen, and M. Ziefle, "Conditional privacy: Users' perception of data privacy in autonomous driving." in *VEHITS*, 2019, pp. 352–359.

[12] E. Carbone and G. Loewenstein, "Dying to divulge: The determinants of, and relationship between, desired and actual disclosure," *Desired and Actual Disclosure*, 2020.

[13] R. Chakraborty, C. Vishik, and H. R. Rao, "Privacy preserving actions of older adults on social media: Exploring the behavior of opting out of information sharing," *Decision Support Systems*, vol. 55, no. 4, pp. 948–956, 2013.

[14] D. Chang, E. L. Krupka, E. Adar, and A. Acquisti, "Engineering information disclosure: Norm shaping designs," in *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, 2016, pp. 587–597.

[15] J. Chen, C. S. Gates, N. Li, and R. W. Proctor, "Influence of risk/safety information framing on android app-installation decisions," *Journal of Cognitive Engineering and Decision Making*, vol. 9, no. 2, pp. 149–168, 2015.

[16] E. K. Choe, J. Jung, B. Lee, and K. Fisher, "Nudging people away from privacy-invasive mobile apps through visual framing," in *Proceedings of IFIP Conference on Human-Computer Interaction*, 2013, pp. 74–91.

[17] A. Chowdhury, G. Karmakar, J. Kamruzzaman, A. Jolfaei, and R. Das, "Attacks on self-driving cars and their countermeasures: A survey," *IEEE Access*, vol. 8, pp. 207 308–207 342, 2020.

[18] E. Commission, "Connected and automated mobility," https://digital-strategy.ec.europa.eu/en/policies/connected-and-automated-mobility, 2020.

[19] L. F. Cranor, "Necessary but not sufficient: Standardized mechanisms for privacy notice and choice," *J. on Telecomm. & High Tech. L.*, vol. 10, pp. 273–308, 2012.

[20] J. C. Duchi, M. I. Jordan, and M. J. Wainwright, "Local privacy and statistical minimax rates," in *Foundations of Computer Science (FOCS), 2013 IEEE 54th Annual Symposium on*. IEEE, 2013, pp. 429–438.

[21] C. Dwork, "Differential privacy," in *ICALP*, 2006, pp. 1–12.

[22] B. Fabian, T. Ermakova, and T. Lentz, "Large-scale readability analysis of privacy policies," in *Proceedings of the International Conference on Web Intelligence*, 2017, pp. 18–25.

[23] N. Gerber, P. Gerber, and M. Volkamer, "Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior," *Computers & Security*, vol. 77, pp. 226–261, 2018.

[24] S. Ghane, A. Jolfaei, L. Kulik, K. Ramamohanarao, and D. Puthal, "Preserving privacy in the internet of connected vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 8, pp. 5018–5027, 2020.

[25] O. Goldreich, "Secure multi-party computation," *Manuscript. Preliminary version*, vol. 78, 1998.

[26] E. B. Goldstein and J. Brockmole, *Sensation and perception*. Cengage Learning, 2016.

[27] R. L. Goldstone, J. R. de Leeuw, and D. H. Landy, "Fitting perception in and to cognition," *Cognition*, vol. 135, pp. 24–29, 2015.

[28] L. Green, N. Fristoe, and J. Myerson, "Temporal discounting and preference reversals in choice between delayed outcomes," *Psychonomic Bulletin & Review*, vol. 1, no. 3, pp. 383–389, 1994.

[29] L. Green and J. Myerson, "A discounting framework for choice with delayed and probabilistic rewards." *Psychological Bulletin*, vol. 130, no. 5, pp. 769–792, 2004.

[30] I.-H. Hann, K.-L. Hui, S.-Y. T. Lee, and I. P. Png, "Overcoming online information privacy concerns: An information-processing theory approach," *Journal of Management Information Systems*, vol. 24, no. 2, pp. 13–42, 2007.

[31] Innovation and N. E. A. INEA, "Intelligent transport systems (its) for road," https://ec.europa.eu/inea/sites/default/files/cefpub/cef_transport_its-2019-web.pdf, 2019.

[32] C. Klauer, T. A. Dingus, V. L. Neale, J. D. Sudweeks, D. J. Ramsey *et al.*, "The impact of driver inattention on near-crash/crash risk: An analysis using the 100-car naturalistic driving study data," 2006.

[33] S. Kokolakis, "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon," *Computers & Security*, vol. 64, pp. 122–134, 2017.

[34] N. K. Malhotra, S. S. Kim, and J. Agarwal, "Internet users' information privacy concerns (iuipc): The construct, the scale, and a causal model," *Information Systems Research*, vol. 15, no. 4, pp. 336–355, 2004.

[35] A. Mathur, M. Kshirsagar, and J. Mayer, "What makes a dark pattern... dark? design attributes, normative considerations, and measurement methods," in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 2021, pp. 1–18.

[36] A. M. McDonald and L. F. Cranor, "The cost of reading privacy policies," *ISJLP*, vol. 4, p. 543, 2008.

[37] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, "Communication-efficient learning of deep networks from decentralized data," in *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics*, 2017, pp. 1273–1282.

[38] H. Nissenbaum, *Privacy in context: Technology, policy, and the integrity of social life*. Stanford, CA: Stanford University Press, 2009.

[39] K. Nissim and A. Wood, "Is privacy privacy?" *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, vol. 376, no. 2128, 2018.

[40] P. A. Norberg, D. R. Horne, and D. A. Horne, "The privacy paradox: Personal information disclosure intentions versus behaviors," *Journal of Consumer Affairs*, vol. 41, no. 1, pp. 100–126, 2007.

[41] M. Nouwens, I. Liccardi, M. Veale, D. Karger, and L. Kagal, "Dark patterns after the gdpr: Scraping consent pop-ups and demonstrating their influence," in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 2020, pp. 1–13.

[42] U. D. of Transportation, "Vehicle-to-infrastructure deployment guidance," https://www.its.dot.gov/factsheets/v2i_guidance.htm, 2019.

[43] K. Olmstead and M. Atkinson, "Apps permissions in the google play store," https://apo.org.au/node/58954, 2015.

[44] L. B. Othmane, H. Weffers, M. M. Mohamad, and M. Wolf, "A survey of security and privacy in connected vehicles," in *Wireless sensor and mobile ad-hoc networks*. Springer, 2015, pp. 217–247.

[45] I. Pollach, "What's wrong with online privacy policies?" *Communications of the ACM*, vol. 50, no. 9, pp. 103–108, 2007.

[46] S. Pötzsch, "Privacy awareness: A means to solve the privacy paradox?" in *IFIP Summer School on the Future of Identity in the Information Society*. Springer, 2008, pp. 226–236.

[47] P. Rajivan and J. Camp, "Influence of privacy attitude and privacy cue framing on android app choices," in *Proceedings of Twelfth Symposium on Usable Privacy and Security (SOUPS)*, 2016, pp. 1–7.
[48] A. Rao, F. Schaub, N. Sadeh, A. Acquisti, and R. Kang, "Expecting the unexpected: Understanding mismatched privacy expectations online," in *Proceedings of Twelfth Symposium on Usable Privacy and Security (SOUPS)*, 2016, pp. 77–96.
[49] J. R. Reidenberg, T. Breaux, L. F. Cranor, B. French, A. Grannis, J. T. Graves, F. Liu, A. McDonald, T. B. Norton, and R. Ramanath, "Disagreeable privacy policies: Mismatches between meaning and users' understanding," *Berkeley Tech. LJ*, vol. 30, pp. 39–88, 2015.
[50] J. R. Reidenberg, N. C. Russell, A. J. Callen, S. Qasir, and T. B. Norton, "Privacy harms and the effectiveness of the notice and choice framework," *ISJLP*, vol. 11, pp. 485–524, 2015.
[51] A. Sarker, H. Shen, M. Rahman, M. Chowdhury, K. Dey, F. Li, Y. Wang, and H. S. Narman, "A review of sensing and communication, human factors, and controller aspects for information-aware connected and automated vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 21, no. 1, pp. 7–29, 2019.
[52] F. Schaub, R. Balebako, A. L. Durity, and L. F. Cranor, "A design space for effective privacy notices," in *Proceedings of Eleventh symposium on usable privacy and security (SOUPS)*, 2015, pp. 1–17.
[53] F. Schaub, B. Könings, and M. Weber, "Context-adaptive privacy: Leveraging context awareness to support privacy decision making," *IEEE Pervasive Computing*, vol. 14, no. 1, pp. 34–43, 2015.
[54] B. Scheibehenne, R. Greifeneder, and P. M. Todd, "Can there ever be too many options? a meta-analytic review of choice overload," *Journal of Consumer Research*, vol. 37, no. 3, pp. 409–425, 2010.
[55] H. A. Simon, "Bounded rationality," in *Utility and probability*. Springer, 1990, pp. 15–18.
[56] H. J. Smith, T. Dinev, and H. Xu, "Information privacy research: an interdisciplinary review," *MIS Quarterly*, pp. 989–1015, 2011.
[57] D. J. Solove, "Introduction: Privacy self-management and the consent dilemma," *Harv. L. Rev.*, vol. 126, pp. 1880–1903, 2012.
[58] A. E. Waldman, "Cognitive biases, dark patterns, and the 'privacy paradox'," *Current Opinion in Psychology*, vol. 31, pp. 105–109, 2020.
[59] J. Walter and B. Abendroth, "On the role of informational privacy in connected vehicles: a privacy-aware acceptance modelling approach for connected vehicular services," *Telematics and Informatics*, vol. 49, no. 101361, 2020.
[60] S. L. Warner, "Randomized response: A survey technique for eliminating evasive answer bias," *JASA*, vol. 60, no. 309, pp. 63–69, 1965.
[61] A. Xiong and R. W. Proctor, "Information processing: The language and analytical tools for cognitive psychology in the information age," *Frontiers in Psychology*, vol. 9, no. 1270, 2018.
[62] A. Xiong, T. Wang, N. Li, and S. Jha, "Towards effective differential privacy communication for users' data sharing decision and comprehension," in *Proceedings of 2020 IEEE Symposium on Security and Privacy (SP)*, 2020, pp. 392–410.