Vision: The Price Should Be Right: Exploring User Perspectives on Data Sharing Negotiations

Jacob Hopkins and Carlos Rubio-Medrano
Texas A&M University - Corpus Christi
{jhopkins2@islander., carlos.rubiomedrano@}tamucc.edu

Cori Faklaris
University of North Carolina at Charlotte
cfaklari@charlotte.edu

***Abstract*—Data is a critical resource for technologies such as Large Language Models (LLMs) that are driving significant economic gains. Due to its importance, many different organizations are collecting and analyzing as much data as possible to secure their growth and relevance, leading to non-trivial privacy risks. Among the areas with potential for increased privacy risks are voluntary data-sharing events, when individuals willingly exchange their personal data for some service or item. This often places them in positions where they have inadequate control over what data should be exchanged and how it should be used.**

To address this power imbalance, we aim to obtain, analyze, and dissect the many different behaviors and needs of both parties involved in such negotiations, namely, the *data subjects*, i.e., the individuals whose data is being exchanged, and the *data requesters*, i.e., those who want to acquire the data. As an initial step, we are developing a multi-stage user study to better understand the factors that govern the behavior of both data subjects and requesters while interacting in data exchange negotiations. In addition, we aim to identify the design elements that both parties require so that future privacy-enhancing technologies (PETs) prioritizing privacy negotiation algorithms can be further developed and deployed in practice.

I. Introduction

Societies have been undergoing a data-driven industrial transformation due to the internet, social media, and Artificial Intelligence (AI) techniques such as Large Language Models (LLMs) [1]. The amount of data that has been consumed and/or created by these technologies has exploded exponentially, as organizations in various sectors are using this gold rush to support their growth [2]. A consequence of these campaigns are the capture of mass data that can identify a real individual or their behaviors, called personal data [3]. This represents a non-trivial privacy risk for nearly all individuals. If we accept Westin's definition of privacy [4], "the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others," then these techniques to collect, store and analyze the large amount of available data, including personal data, potentially violate privacy.

Symposium on Usable Security and Privacy (USEC) 2025
24 February 2025, San Diego, CA, USA
ISBN 979-8-9919276-5-9
https://dx.doi.org/10.14722/usec.2025.23016
www.ndss-symposium.org, https://www.usablesecurity.net/USEC/

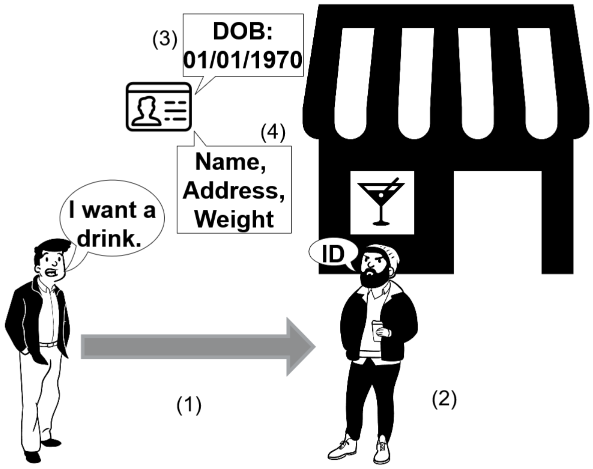

Fig. 1: Our running example featuring a voluntary data-sharing event occurring at a bar: bouncer and patron engage in a negotiation for the release of personal data.

Unfortunately, events that violate privacy are occurring more frequently. Within the context of the U.S., the public has seen the federal government collect mass internet communications [5], attackers stealing personal data from companies [6], companies selling personal data overseas [7], and more. Government, academia and industry are addressing the need for better privacy controls. The European Union's General Data Protection Regulation (GDPR) [3] safeguards the data rights of their citizens. Legislative bills that mirror the GDPR have been gaining support within the U.S. Congress [8]. And multiple services, i.e., Optery [9] and Deleteme [10], have been launched to assist subscribers in removing their personal information from data brokers and the Internet.

While these initiatives have helped to mitigate privacy risks posed by the digitization of our lives, there is work to be done focusing on the privacy risks associated with data collection, specifically voluntary data-sharing events as illustrated in Fig. 1, in which the patron, Bob, is depicted on the left side. In step (1), Bob is approaching the bar. In step (2), Bob meets the bar's bouncer, Tim. Their job as the bar's representative is to ensure that every potential patron is of age to purchase an alcoholic beverage, as is mandated in several countries. In step (3), Bob willingly exchanges some personal data, their date of birth, by producing their identification card to Tim. Three issues can occur in these events that pose an increased privacy risk: (1) the sharing method reveals more data than intended (for example, in step (4) of Fig. 1, Bob's identification card has more data than data of birth); (2) a party of the event acts in bad faith (say Tim collects Bob's data for their own purposes); and/or (3) a power imbalance between the parties.

The figure of Bob the patron and Tim the bouncer is but one example of these voluntary data-sharing events. These types of events occur both in the online setting, i.e., exchanging financial data to shop on an e-commerce site, and in the physical setting, i.e., exchanging personal data and ticket data to ticket booth operator to attend a concert. The main goal of our research is to address the issues of voluntary data-sharing events in both online and physical settings, based on our guiding philosophy that individuals should have a say over how their personal data is used. To that end, our aim is to develop approaches that enable *data subjects* (those whose data is being exchanged) and *data requesters* (those who want to acquire the data) in a voluntary data-sharing event to negotiate what personal data will be exchanged and what will be done with it. Our approaches will meet three goals: (1) Provide greater control over personal data to the data subjects; (2) Enumerate the risks to both the data subjects and data requesters; and (3) Provide greater transparency on how personal data may be used.

To accomplish these goals, we are developing a negotiation framework to enable both data subjects and data requesters to negotiate about what personal data will be shared. We are designing the framework to support three forms of negotiation: manual negotiation, automated negotiation, and semi-automated negotiation, in which autonomous agents provide support to their human counterparts by recommending actions to take during the negotiation. As an initial step, we are designing a multi-stage study that surveys the populations of data subjects and data requesters. The study will gather information from these two populations to inform the framework so that it meets the needs of both populations. Most significantly, we seek to understand what are the sets of personal data elements that data subjects are willing to share to various data requesters under different conditions in order to develop a future negotiation framework. To that end, some sample research questions that will be investigated as part of our study may include, but may not be limited to, the following:

RQ$_1$ *What personal data should be shared to a requester?*
RQ$_2$ *What factors influence the decision to release data?*
RQ$_3$ *What factors influence the decision to request data?*
RQ$_4$ *What data actions are done with personal data?*
RQ$_5$ *What data actions should be allowed to occur to data?*
RQ$_6$ *What is the perceived privacy risk to data subject?*
RQ$_7$ *What is the operational risk to the data requester?*
RQ$_8$ *What controls are needed to support data subjects?*
RQ$_9$ *What controls are needed to support data requesters?*

II. Background

A. Related Works

Over the years, there have been multiple works that developed a negotiation framework for determining what data to disclosure. Bennicke and Langendorfer [11], proposed a negotiation framework for web applications based around the P3P standard which defines privacy policies for service providers and preference document called APPEL that indicates what the users want from the service provider in regards to how the service provider uses their personal data. In addition, Walker, Mercer and Seamons proposed their "Or Best Offer" (OBO) negotiation scheme for web applications [12]. Their design goals for their negotiation scheme were completeness, fair, and secure, making use of agents operating for the both the client and server to drive the negotiation, and establishing various rules that the agents need to follow to ensure fairness. In a similar manner, Ukil et al. [13] proposed a negotiation scheme for an Internet of Things (IoT) platform based on a set of privacy policies. Both parties will follow the appropriate policies to either publish their data as in the case of the data producer or request that data as in the case of the data requester. Once the negotiation process is complete and what data is to be exchanged is defined, a set of privacy preserving rules is be created for the data consumer to access the data. Moreover, Jung and Park proposed a market-based negotiation framework for selling differentially-private data [14]. The basis of this framework is to find and match data providers and data consumers that will exchange differentially private data at a negotiated ϵ value and price point, using the Rubinstein bargaining [15] type negotiation. Furthermore, Filipczuk et al. [16] proposed a novel multi-issue automated negotiation framework to negotiate privacy permissions using their "partial-complete offer" protocol. They evaluated their framework with a user study and demonstrated that their framework produced outcomes that better aligned with the users' privacy preferences compared to the standard "take-it-or-leave-it" approach.

B. Personal Data

GDPR defines personal data as "Any information relating to an identified or identifiable natural person ('data subject')" where 'identifiable natural person means "one who can be identified, directly or indirectly, in particular by reference to an identifier" [3]. However, as technology has evolved so has the potential for new kinds of data produced or inferred. Social media has made it possible to determine a person's relationship circle, personal images, and location check-ins [17]. IoT devices are able to gather new type of data ranging from health data to location data to device data [17]. Often this data is collected, analyzed, and sold by data brokers to other third party entities [18]. This data from these new sources can be further leveraged to produce more data that is potentially of higher personal value such as voting behaviors [19] by being analyzed with powerful analysis tools such as deep learning models [17]. To understand this evolution of personal data, Saglam, Nurse and Hodges developed several taxonomies that classified both the current and new categories of personal data [17]. In particular they focused on both the financial and health sectors. They produced taxonomies of the personal data that are used in these sectors from the viewpoints of industry, academia, and the government sectors, and found that the government was significantly behind of what academia and industry viewed as personal data [17].

C. Privacy Risk

In order to calculate the potential privacy risks involved in data sharing events, the following need to be considered: (1) What harms occur when there is a privacy violation; (2) What are the threats or actions that cause a privacy violation; (3) What factors affect how an individual perceives privacy risk thus affecting how one is willing to share their personal data.

1) Harms and Actions: Citron and Solove [20] enumerated a privacy harm topology in which they identified several different categories, including physical, economical, reputational, psychological, discrimination, etc. Moreover, Brooks et al. [21] argue that privacy risks differ from information security risks, which come from threats that are not authorized to access the asset thereby compromising the asset's confidentiality, integrity, or availability. However, privacy risks come from threats who are potentially authorized to access the personal data, but the action that the threat performs on the data is perceived as causing some privacy harm by the data subject. Brooks et al describe these privacy threats as "problematic data actions" to distinguish them from traditional threats [21].

2) Relevant Factors: One of the core issues of perceived privacy risk is the privacy paradox, which describes the phenomenon where users' stated preferences is to preserve the privacy of their personal data but their revealed preferences are more relaxed. Thus users are more willing to share or sell their data in practice [22]. One possible explanation for this discrepancy is that benefits to the data subject in sharing their personal data far exceeds the costs incurred. Bhatia and Breaux [23] explored the factors that could influenced the decision process that data subjects undergo in determining whether or not to share their data. They modeled the data subjects' perceived privacy risk as the willingness to share their personal data and identified 6 different factors that affect an individual's willingness to share: data type, computer type, data purpose, privacy harm, harm likelihood, and individual demographic factors. Also, Dupree et al. [24], sought to identify how users differ in their behaviors towards privacy and security practices by identifying 5 different clusters of users in relation to their privacy and security practices.

III. Proposed Methodology

A major limitation of the works presented in Sec. II-A is the lack of insights on how both data subjects and data requesters interact with each other within a negotiation on personal data, including what design requirements each party wants from a negotiation framework. Thus, to address this limitation, we propose a user study to investigate both sides of the data negotiation process using techniques developed from the usable security and privacy domains. This section will detail the proposed plan by identifying the populations that will be surveyed, the selection of research questions, the structure of the study, and the expected results of the study and how those results will be integrated back into a future negotiation framework.

A. Targeted Population

As mentioned before, within the privacy negotiation setting, there are at least two parties that engage in this interaction: the data subjects and the data requesters. With this framing, we can determine what populations would inhabit these roles in the negotiation event.

In terms of limitations for participant recruitment, we restrict the selection of individuals to that of the United States population. The reason for this limitation is to maintain a consistent cultural understanding of privacy and privacy harms. The foundation of the future negotiation framework is based on a theory of privacy harm that originates from a United States legal context [20]. It would be inappropriate to recruit from populations outside the US because of their different cultural understandings of privacy and harms. For the role of data subjects, we are targeting the general US population because this is the population that is exchanging their personal data for access to a service or product. For the role of data requesters, we are targeting the individuals who either directly handle the data subject's personal data, i.e. front-line workers such as in-take nurses, bar bouncers, ticket booth operators, and individuals that design and operate the data security measures, i.e. IT professionals operating the data security or privacy operations for an organization. These potential participants will be recruited from businesses, non-profit organizations, and online vendors because these are the entities that are offering a service or product for access to the personal data of their users in addition to other resources, i.e., money.

B. Research Questions

As stated previously, this study's goal is to determine what is required for a future negotiation framework from the perspective of both parties in the negotiation. To achieve this goal, we introduced 9 research questions in Sec. I. We now elaborate on the nature of each of these questions. The core of the negotiation framework is the determination of what is the appropriate set of personal data that should be shared in a given set of contexts, i.e., what personal data should Bob share with Tim to get a drink. This exchange is based on the concept of information flows from Nissenbaum's contextual integrity theory of privacy [25].

1) Handling of Personal Data: To determine what is that set of personal data items, RQ_1 and RQ_2 should be posed to the data subject population. The most straightforward manner to investigate RQ_1 and RQ_2 from the data subject perspective would be as a series of scenario based questions where participants can select which pieces of personal data they would share given a set of factors. From the bar example in Fig. 1, Bob would be asked what data he would prefer to exchange and for what reason did he select that particular set of data. RQ_3 should be posed to the data requester population. From the perspective of data requesters, they experience a different set of obligation from the data subjects, i.e., Tim and the bar have legal and business obligations to collect personal data of their customers to operate properly.

2) Data Actions: Another aspect to investigate is that of acceptable data actions. A critical component of a future negotiation framework will be its privacy risk model where the threats will be modeled as problematic data actions [21]. Thus it is important to establish what is the range of data actions that data requesters currently do with the shared data, i.e., what action does the bar do with Bob's data. It also important to determine what potential privacy harms these actions could be perceived to incur, i.e., how does the bar's actions potentially violate Bob's privacy. It also necessary to investigate what actions are data subjects are willing to allow for a personal data item, i.e., what is Bob's preference for the set of actions the bar can perform on his data. RQ$_4$ and RQ$_5$ seeks to collect these answers from data requesters and data subjects respectively.

3) Risks of Negotiation: RQ$_6$ and RQ$_7$ are related to the risk model within the negotiation framework. To introduce transparency into negotiation process, a future negotiation framework needs to be designed to compute the risks involved in sharing specific data elements from personal data. For example, Bob and the bar should both know the potential risks to Bob's privacy if data is shared and the bar's risk if data is not shared in order to have a transparent negotiation. RQ$_6$ will be posed to data subjects and RQ$_7$ will be posed to requesters.

4) Usability of Negotiation Framework: RQ$_1$ to RQ$_7$ are exploring how specific functions within a future negotiation framework should compute optimal sets of personal data and the associated risks of those sets so that both parties achieve their desired outcomes in the negotiation. RQ$_8$ and RQ$_9$ differ from the previous questions in that they are used to investigate how a future negotiation framework should be designed to provide usable controls to users. From Whitten and Tygar's work, we know that typical users are not motivated to engage with security controls that require maintenance and upkeep; they just want it to work [26]. However, there are users who are more motivated to engage with security and privacy practices [24]. To be readily adopted, a future negotiation framework needs to be usable for various categories of users. RQ$_8$ and RQ$_9$ will be used to capture that information.

C. Survey Design

With the targeted populations identified for the study and the reasons for the selection of the research questions, the user study can be tailored to ask specific interview questions to each population. As shown in Fig. 2 the user study will be split into three different tracks, one entirely focused on the data subject perspective, one purely focused on the data requester perspective, and one centered on the usable design portions. As the proposed study includes the recruitment of human subjects, we will submit it to our Institutional Review Board (IRB) for approval before conducting the study. All data collected from this study will be protected and anonymized.

1) Data Subject Track: Since RQ$_1$, RQ$_2$, RQ$_5$, and RQ$_6$ need to be answered from the data subject population, these questions will be addressed by the data subject track as outlined in Fig. 2. The data subject survey track will be conducted online to recruit as many individuals as possible and from as broad a range as possible. The surveys will be created using a survey management service, i.e. Qualtrics, to achieve this. The anticipated number of participants recruited for this track ranges from 800 to 1000 participants. The majority of participants will be recruited through a crowd-sourcing platform such as Amazon's MTurk platform, but we will manually recruit individuals if necessary through advertisement or email messaging. The data subject track consists of three phases: pre-test, survey, and post-test phases.

a) Pre-Test Phase ①: This phase will consist of an initial assessment of participants to categorize them into one of several possible privacy personas. The purpose of this assessment is to determine the range of data a persona is willing to share and what factors affect those preferences. The assessment will be mechanically similar to that of Westin's Privacy Segmentation Index [27] [28], but will use Dupree et al. privacy personas [24] as the foundation for the assessment.

b) Survey Phase ②: For this phase, the vignette survey format was selected as the core approach. A vignette survey use descriptions of scenarios combined with differing level of important characteristics called dimensions to explore the respondents' judgments to those scenarios [29]. Bhatia and Breaux used a vignette survey to determine what factors affected users' perceived risk computation and the significance of those factors [23]. Our study will take inspiration from this work, but it differs by determining what sets of personal data items users are willing to share under various factors, i.e., business type, data actions, etc. Other factors will be identified to be used in the survey through analysis of current privacy and data policies of businesses and corporations.

c) Post-Test Phase ③: To finish this track of the study, this phase will finish with a demographic survey to collection demographic information such as age, gender, ethnicity, etc.

2) Data Requester Track: RQ$_3$, RQ$_4$, and RQ$_5$ are needed to be answered from the data requester population and the proposed format can be viewed in Fig. 2 in the data requester track. This track consists of the following two phases:

a) Exploratory Phase ④: This phase will explore the initial view of the business and corporate requirements for personal data through published privacy or data policies. Analyzing these policies will assist in the creation of potential questions to ask to recruited data requester participants.

b) Survey Phase ⑤. The second phase of this track is the survey phase. There is a potential point of failure that can occur with this particularly target population. The population that is being targeted, front-line workers and IT professionals of businesses, organizations, etc., is a significantly smaller pool of potential candidates. Thus, to address this potential shortcoming, we will use a semi-structured interview format. The number of participants to be recruited for this track of the study will be between 20 and 40 individuals. The interviews will be conducted in whatever manner that is most convenient for the participant either in-person or remotely. The interviews will last up to 45 minutes to an hour. This purpose

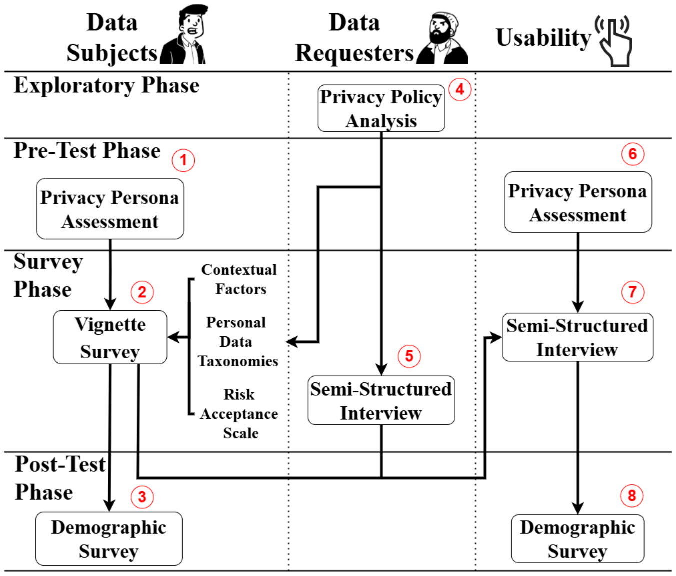

Fig. 2: Our proposed study design comprising three tracks and four different interconnected phases.

of these interviews is to gather information about the business needs concerning the collection of personal data, potential obligations, i.e. legal, to collect personal data, risks to the business if that data is not collected, how data collection and data privacy policies are implemented, etc.

3) Usability Track: The last track, the usability track in Fig. 2, will be used to investigate RQ_8 and RQ_9. The usability track will recruit participants from both populations. The number of participants recruited for this study will range from 20 to 40 individuals. This track consists of the following:

a) Pre-Test Phase ⑥: This phase will also conduct a privacy persona assessment of the participants same as the one conducted in the pre-test phase of the data subjects track. Participants from both the data subject population and data requester population will complete the assessment.

b) Survey Phase ⑦: Since the specified research questions for this track are exploring potential design requirements in a future negotiation framework, the survey phase will use a semi-structure interview format similar to what was discussed in the data requester track. Additionally, the results gathered from the data subject and requester tracks' surveys will be used to develop the interview questions in this phase.

c) Post-Test Phase ⑧: To end this track, this phase will also conduct a demographic survey to collect various demographic data such as age, gender, ethnicity, etc.

D. Expected Results

Having described the structure of our study, it is necessary to determine what type of results are expected and how they may be incorporated back into the negotiation framework.

From the data subject portion of the study, we anticipated two sets of results. The first set of results that are anticipated are sets of personal data items and allowed data actions that the participatory data subjects selected during the course of the survey for various scenarios. A planned part of the future negotiation framework is a recommendation system that will suggest what personal data elements and what data actions should be given to the data requester during the course of a negotiation. The sets collected during the survey will act as training data to develop the recommendation system. The second set of results will be the identification of which contextual factors that influenced the data subjects' perceived risk of individual data elements and the factors' significance in that process. These factors and their importance will be used to update the perceived privacy risk model of the framework.

From the data requester portion of the study, we anticipate three set of results. Similar to the the first set of results from the data subjects, the first set of results from the data requesters are sets of personal data elements and data actions that the data requesters require for their operations. Once again, another recommendation system will be developed using this set of data as training data so that the recommendation system will produced recommended data requests for the requester's organize type. The second set of results are the different categories of data actions that are currently being used to collect and process personal data. These results will be used to update the perceived privacy risk model and the negotiation algorithms. The third anticipated result is the set of potential operational risks that a data requester could be exposed to if they don't obtain access to required personal data, which will be used to update the operational risk model in our framework.

From the usability portion of the study, we anticipate receiving two sets of design requirements and recommendations that will be used to re-design elements of the negotiation framework and to design the interfaces through which the users, both data subjects and requesters, will interact with it.

IV. Conclusion and Future Work

Data is a significantly important resource in the world's economies today; thus highly sought after to the point of potential privacy violations. This work seeks to remedy this issue by developing a privacy negotiation framework that mediates what personal data elements should shared from a data subject to a data requester. Our first step is the creation of a user study to investigate how data subjects and data requesters interact with one another in a negotiation, which is a still a work in progress. For future work in the mid-term, the results of our study will be incorporated back into the design of a future negotiation framework, which will be evaluated through a user study. Finally, for long-term future work, different cultural perspectives of privacy harms and legal frameworks, i.e. GDPR, will be also incorporated.

Acknowledgments

This work was partially supported by the National Science Foundation (NSF) under Grants No. 2232911 and No. 2131263, and by a SAGE Scholarship from Texas A&M University - Corpus Christi. Faklaris is supported by NSF Grant No. 2346281, DOD Department of the Army (DA) Grant No. W911NF2410189, Google, and BasisTech founder Carl Hoffman.

References

[1] V. Dhar, "The paradigm shifts in artificial intelligence," *Communications of the ACM*, vol. 67, no. 11, p. 50–59, Oct 2024.

[2] H. N. Chua, J. S. Ooi, and A. Herbland, "The effects of different personal data categories on information privacy concern and disclosure," *Computers & Security*, vol. 110, p. 102453, 2021.

[3] European Parliament and Council of the European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council.

[4] A. F. Westin, "Privacy and freedom," *Washington and Lee Law Review*, vol. 25, no. 1, p. 166, 1968.

[5] T. Sottek and J. Kopfstein, "Everything you need to know about prism," *The Verge*, July 2013.

[6] L. Franceschi-Bicchierai, "Hacker leaks millions more 23andme user records on cybercrime forum," *TechCrunch*, Oct 2023.

[7] E. Jennings-Trace, "The us government is cracking down on firms selling user data to these countries," *TechRadar*, Oct 2024.

[8] C. McMorris Rodgers, "American privacy rights act of 2024," 06 2024.

[9] "Optery," Nov 2024. [Online]. Available: https://www.optery.com/

[10] "Deleteme," Nov 2024. [Online]. Available: https://www.deleteme.com/

[11] M. Bennicke and Langendorfer, "Towards automatic negotiation of privacy contracts for internet services," in *The 11th IEEE International Conference on Networks, 2003. ICON2003.*, 2003, pp. 319–324.

[12] D. D. Walker, E. G. Mercer, and K. E. Seamons, "Or best offer: A privacy policy negotiation protocol," in *2008 IEEE Workshop on Policies for Distributed Systems and Networks*, 2008, pp. 173–180.

[13] A. Ukil, S. Bandyopadhyay, J. Joseph, V. Banahatti, and S. Lodha, "Negotiation-based privacy preservation scheme in internet of things platform," in *Proc. of the First Int. Conf. on Security of Internet of Things*, ser. SecurIT '12. New York, NY, USA: ACM, 2012, p. 75–84.

[14] K. Jung and S. Park, "Privacy bargaining with fairness: Privacy-price negotiation system for applying differential privacy in data market environments," in *2019 IEEE Int. Conf. on Big Data (Big Data)*, 2019, pp. 1389–1394.

[15] A. Rubinstein, "Perfect equilibrium in a bargaining model," *Econometrica*, vol. 50, no. 1, pp. 97–109, 1982. [Online]. Available: http://www.jstor.org/stable/1912531

[16] D. Filipczuk, T. Baarslag, E. H. Gerding, and m. c. schraefel, "Automated privacy negotiations with preference uncertainty," *Autonomous agents and multi-agent systems*, vol. 36, no. 2, 2022.

[17] R. Belen Saglam, J. R. Nurse, and D. Hodges, "Personal information: Perceptions, types and evolution," *Journal of Information Security and Applications*, vol. 66, p. 103163, 2022.

[18] H. Oh, S. Park, G. M. Lee, H. Heo, and J. K. Choi, "Personal data trading scheme for data brokers in iot data marketplaces," *IEEE Access*, vol. 7, pp. 40 120–40 132, 2019.

[19] C. Cadwalladr and E. Graham-Harrison, "Revealed: 50 million facebook profiles harvested for cambridge analytica in major data breach," Mar 2018.

[20] D. K. Citron and D. J. Solove, "Privacy harms," *Boston University law review*, vol. 102, no. 3, pp. 793–863, 2022.

[21] S. Brooks, M. Garcia, N. Lefkovitz, S. Lightman, and E. Nadeau, "An introduction to privacy engineering and risk management in federal information systems," 2017-01-05 2017.

[22] A. Acquisti and J. Grossklags, "Privacy and rationality in individual decision making," *IEEE Sec. & Privacy*, vol. 3, no. 1, pp. 26–33, 2005.

[23] J. Bhatia and T. D. Breaux, "Empirical measurement of perceived privacy risk," *ACM Trans. Comput.-Hum. Interact.*, vol. 25, no. 6, Dec. 2018.

[24] J. L. Dupree, R. Devries, D. M. Berry, and E. Lank, "Privacy personas: Clustering users via attitudes and behaviors toward security practices," in *Proc. of the 2016 Conf. on Human Factors in Computing Systems*, ser. CHI '16. New York, NY, USA: ACM, 2016, p. 5228–5239.

[25] H. F. Nissenbaum, *Privacy in context: technology, policy, and the integrity of social life*, 1st ed. Stanford Law Books, 2010.

[26] A. Whitten and J. D. Tygar, "Why johnny can't encrypt: A usability evaluation of PGP 5.0," in *8th USENIX Security Symposium)*, Aug 1999.

[27] A. F. Westin, "E-commerce & privacy: What net users want," *Privacy & American Business*, 1998.

[28] P. Kumaraguru and L. F. Cranor, "Privacy indexes: a survey of westin's studies," 2005. [Online]. Available: http://reports-archive.adm.cs.cmu.edu/anon/anon/home/ftp/usr0/ftp/isri2005/CMU-ISRI-05-138.pdf

[29] C. Atzmüller and P. M. Steiner, "Experimental vignette studies in survey research," *Methodology*, vol. 6, no. 3, pp. 128–138, 2010.