



Beyond the Privacy–Security Trade-Off: How Data Sensitivity, Time, and Trust Shape Individuals’ Willingness to Disclose Information

Tianqi Hu

Nanjing Foreign Language School Xianlin Campus, Nanjing, China
constanthuu@gmail.com

Abstract. This paper examines how individuals’ willingness to trade privacy for security is influenced by factors beyond the traditional model. Using data from the Pew Research Center and other authoritative institutions, the study uses descriptive statistics and comparative analysis to explore the impact of data intrusiveness, generational differences, temporal decay, and perceived legitimacy on individuals’ privacy preferences. The findings of this essay show that individuals’ willingness to trade privacy for security is not static, but rather depends on the sensitivity of data, changes in urgency over time, trust in data-collecting institutions, and age-related differences in attitudes toward privacy. This study contributes to a more nuanced understanding of privacy decision-making by integrating multiple contextual and psychological variables into a unified analytical framework. It also provides empirical implications for policymakers seeking to balance security measures with public acceptance in modern societies. The results of this essay challenge the traditional trade-off model, reflecting that people’s willingness to give up privacy for security is dynamic and context-dependent.

Keywords: Data Intrusiveness, Temporal Dynamics, Generational Differences, Legitimacy

1 Introduction

In modern society, individuals must balance privacy and security. After the September 11 terrorist attacks on the World Trade Center and the Pentagon, the U.S. government implemented multiple surveillance measures to locate terrorists and prevent further attacks. Though these measures enhanced national security, they also created serious concerns about individual privacy. In the traditional trade-off model, researchers summarized the relationship between privacy and security as a simple trade-off relationship and failed to consider the influence of multiple factors on individuals’ privacy decisions. Other factors, including data intrusiveness, time decay, generational variations, and perceived legitimacy, also influence individuals’ decisions. Therefore, this essay focuses on how different factors shape individuals’ willingness to trade

privacy for security, beyond the traditional trade-off model. This essay aims to explore the extent to which individuals' willingness to trade privacy for security is influenced by multiple factors.

2 Methodology

Secondary data analysis, which originated from the Pew Research Center and other academic institutions, was used in this research. The study uses descriptive statistics to summarize the patterns of individuals' willingness to trade privacy for security under the influence of data intrusiveness, time decay, age variations, and perceived legitimacy. Moreover, the study uses comparative analysis to compare the differences between different times, ages, and data types. Lastly, visual representations were also used to illustrate the combined effects of multiple factors on individuals' willingness. Specifically, bar charts, tables, and line charts were drawn to allow for an intuitive comparison.

3 Traditional Privacy–Security Trade-off Model

3.1 Privacy-Security Trade-off Theory

The traditional model, as discussed by Daniel J. Solove, often states that there is a trade-off relationship between privacy and security [1], as Solove explains, “the common argument is that privacy and security are in tension, and that to increase one, people must decrease the other.” In this model, privacy was seen as an obstacle to security, and the increase of one of them leads to the decrease of the other one. This model was further strengthened by privacy calculus theory, which treats privacy disclosure as a cost-benefit decision. Dinev and Hart argue that individuals' privacy decisions are shaped by their evaluation of perceived benefits and risks [2].

3.2 Limitations of the Traditional Model

However, this model is oversimplified, as individuals' willingness to give up privacy was also influenced by the temporal decay of public support, generational differences, and the varying intrusiveness of different types of data.

4 Beyond the Traditional Trade-off Model

4.1 Data Sensitivity and Perceived Intrusiveness

The traditional model overlooks the intrusiveness of data. According to the Pew Research Center [3], individuals generally consider that the government collecting data about all Americans to assess potential terrorist threats is acceptable, while far fewer individuals accept the government accessing users' audio to help criminal investigations. Therefore, this contrast highlights that individuals do not perceive all forms of privacy loss equally. Instead, the willingness to give up privacy decreases as

the intrusiveness of data collected increases. One possible explanation of such a contrast is that more intrusive forms of data are perceived as greater threats to personal autonomy, showing that the extent to which individuals are willing to trade privacy for security is influenced by the type of data collected.

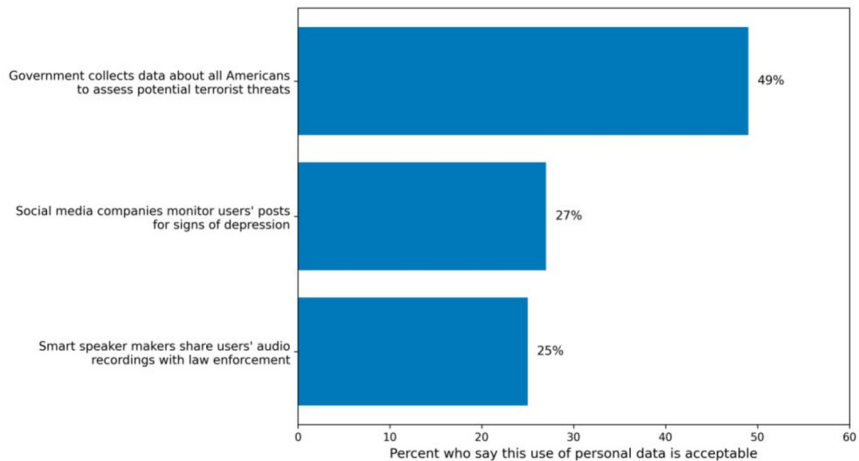


Fig 1. Public acceptance declines as data access becomes more intrusive (Picture credit: original).

Figure 1 compares public acceptance of different uses of personal data, showing that broader data collection for terrorist-threat assessment receives higher acceptance than more content-specific data access, such as monitoring social media posts or sharing smart-speaker audio recordings with law enforcement. Chart created by the author based on data from Pew Research Center [3].

Similarly, the research down by Markos, Labrecque, Milne etc. states that both information type and exchange partner context impact sensitivity perceptions, and willingness to disclose personal information [4].

4.2 Temporal Decay of Public Support for Surveillance

Another factor that affects individuals' willingness to give up privacy for security is time decay. According to the Pew Research Center [5], in the years following the September 11 attacks, public concern about national security was relatively high, and thus more individuals were willing to support surveillance measures. However, over time, public support for these policies decreased as the immediate threats diminished. Specifically, the percentage of individuals who favor the measurement that required citizens to carry national IDs decreased from 70% to 57%, and the percentage of individuals' support for the government's monitoring of personal phone calls decreased from 33% in August 2002 to 29% in August 2011.

Table 1: Declining Public Support for Anti-Terrorism Surveillance Measures, 2001–2011

Measure to curb terrorism	Sept. 2001 (%)	Aug. 2002 (%)	Dec. 2006 (%)	Aug. 2011 (%)
Requiring that all citizens carry a national ID card at all times	70	59	57	57
Extra airport checks on passengers who appear to be of Middle-Eastern descent	—	59	57	53
Government monitoring credit card purchases	—	43	42	42
Government monitoring personal phone calls and emails	—	33	34	29

Table 1 shows changes in public support for requiring national ID cards, extra airport checks, credit card monitoring, and monitoring of personal phone calls and emails. Data adapted from Pew Research Center [5].

This suggests that individuals' willingness to sacrifice privacy is also tied to the temporal change. When the security threats are salient, the willingness to give up privacy increases; as the salience of security threats decreases, the demand for privacy reemerges. This indicates that individuals' willingness to give up privacy for security is not stable, but rather fluctuates over time.

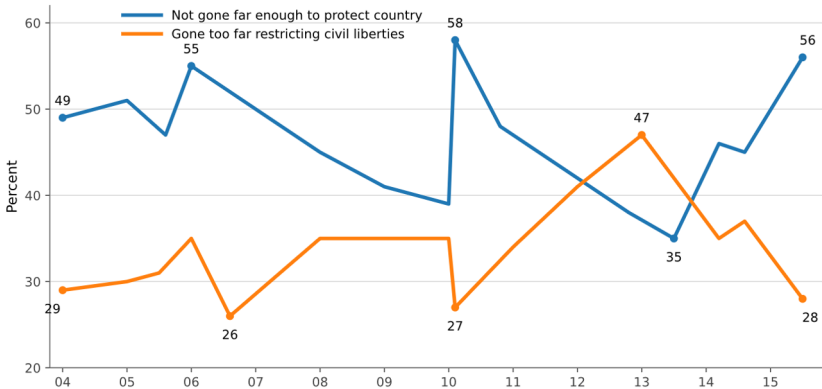


Fig 2. Shifting public concerns between national security and civil liberties over time (Picture credit: original).

The blue line in Figure 2 represents the percentage of respondents who believed that anti-terrorism policies had not gone far enough to protect the country, while the orange line represents the percentage who believed that such policies had gone too far in restricting civil liberties. Data adapted from Pew Research Center [6].

4.3 Generational Differences in Privacy Preferences

Moreover, age also plays an important part in how much privacy individuals are willing to give up for security.

Overall, younger individuals are more concerned about privacy, so they are less likely to give up their privacy. For example, after the San Bernardino attack, the US government asked Apple to unlock the suspect's phone. Younger individuals generally

did not support this proposal, while older individuals tended to have more support for the proposal, showing that younger generations place greater importance on their privacy, and older generations are usually more willing to give up privacy [7].

The reason why the attitudes to security and privacy were not uniform is that the young individuals were influenced by different life experiences, familiarity with technology, and different levels of trust in government. Older individuals, who may prioritize security and safety over privacy, may demonstrate higher levels of support for surveillance, but younger generations, who are more aware of digital risks, are more likely to oppose this intrusion. Thus, the trade-off between privacy and security varies across demographic groups.

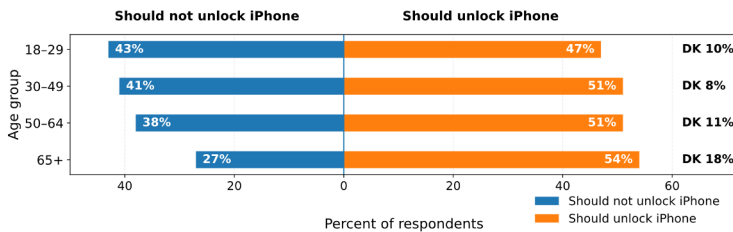


Fig 3. Generational differences in views on the Apple iPhone unlocking dispute (Picture credit: original).

Figure 3 compares support for the Justice Department and support for Apple across age groups, showing that older adults were more likely to support government access, while younger adults were more divided. Data adapted from Pew Research Center [7].

4.4 The Role of Legitimacy in Privacy Disclosure

Legitimacy is also a key factor in shaping individuals' willingness to give up privacy for security. The graph below was drawn according to Meng, Li, & He's [8] research on the individuals' willingness to give up their privacy for security during the Shanghai COVID-19 lockdown. The research found that when individuals perceive the data collector as legitimate, their willingness to disclose private data would increase. To be specific, the standardized coefficient(β) of direct effect on disclosure is 0.48, and the standardized coefficient(β) of cognitive legitimacy is 0.33. Moreover, to exclude that this increase in willingness is caused by factors like altruism, researchers investigated the impact of altruism on the willingness to disclose and found that the standardized coefficient(β) of the effect of altruism on altruism of moral legitimacy and cognitive legitimacy are 0.18 and 0.16, respectively, and the standardized coefficient(β) of the mediator effect is 0.08. Therefore, they calculated the standardized coefficient(β), which is 0.03, showing that the indirect influence on disclosure by legitimacy through altruism is relatively low.

This finding suggests that individuals' choice to give up privacy was also influenced by the trustworthiness of the data-collecting institutions. In other words, when the legitimacy of data collectors increases, individuals' willingness to accept intrusions increases, even when the data is sensitive.

Moreover, the indirect effect of legitimacy through other factors, such as altruism, is relatively low, suggesting individuals tend to make privacy decisions based on concrete trust in institutions, rather than abstract ideological commitment.

Therefore, legitimacy also acts as a factor in shaping individuals' willingness to sacrifice privacy in exchange for security, further demonstrating that the trade-off between privacy and security also correlates with psychological factors instead of pure cost-benefit calculations.

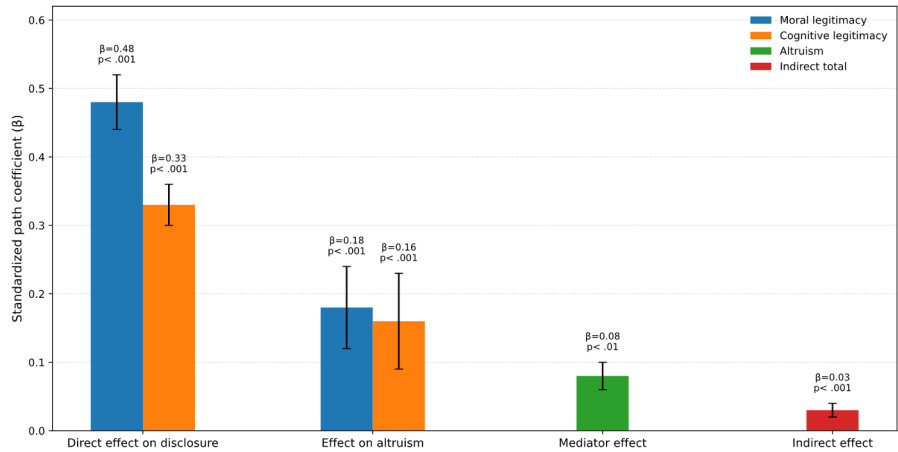


Fig 4. Effects of legitimacy on privacy disclosure. (Picture credit: original)

As shown in figure 4, Beta values represent standardized path coefficients, showing that moral legitimacy and cognitive legitimacy are positively associated with privacy disclosure, while the indirect effect through altruism is relatively small. Recreated based on findings reported by Meng, Li, and He [8].

This finding is similar to Kehr et al.'s privacy-calculus model, which states that significant relationships were found between general privacy concerns and perceived risks, general institutional trust and perceived benefits, and sensitivity and perceived risks and benefits. [9]

5 Discussion

5.1 Age Differences Across Levels of Data Intrusiveness

This paper found that younger individuals are less willing to trade privacy for security compared with older individuals, and this paper found that individuals' support for surveillance declined over time. After due consideration, this paper raised a question: whether age influences individuals' willingness to give up the privacy of different levels of intrusiveness. It is hypothesized that older individuals are more willing to give up

privacy when both the intrusiveness is high and low, since they generally emphasize safety more than young individuals [10].

According to the research data of Pew, a bar chart was constructed to compare younger individuals' and older individuals' acceptance of surveillance measures with different levels of intrusiveness. In this chart, older individuals have higher levels of acceptance of surveillance at each level. For example, individuals aged 65+ have an 88% acceptance rate for accessing residential security camera footage, while individuals aged 18-29 have 57% for this category.

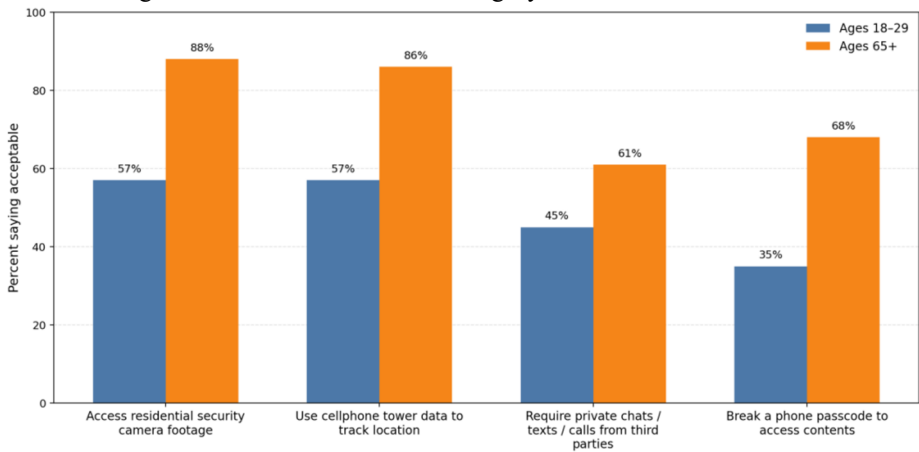


Fig 5. Acceptance of selected law-enforcement surveillance measures by age group. (Picture credit: original)

Figure 5 compares adults aged 18–29 and adults aged 65+ across four surveillance measures, showing that older adults report higher acceptance across all selected measures. Data adapted from Pew Research Center [10].

5.2 Age Differences in Privacy Trade-offs Across Different Purposes

This bar chart shows that younger individuals are more willing to give up privacy for fitness-related purposes but less willing to give up privacy for security-related purposes. Specifically, 52% of individuals aged 18-29 are willing to give up privacy for fitness-related purposes, such as sharing data with medical researchers, compared with 35% of individuals aged 65+; 42% of individuals aged 18-29 are willing to give up privacy for social media monitoring to identify depression and self-harm risk, compared with 18% of individuals aged 65+. However, 58% of individuals aged 65+ support DNA testing companies sharing genetic data with law enforcement, which is significantly higher than 39% of individuals aged 18-29 [3].

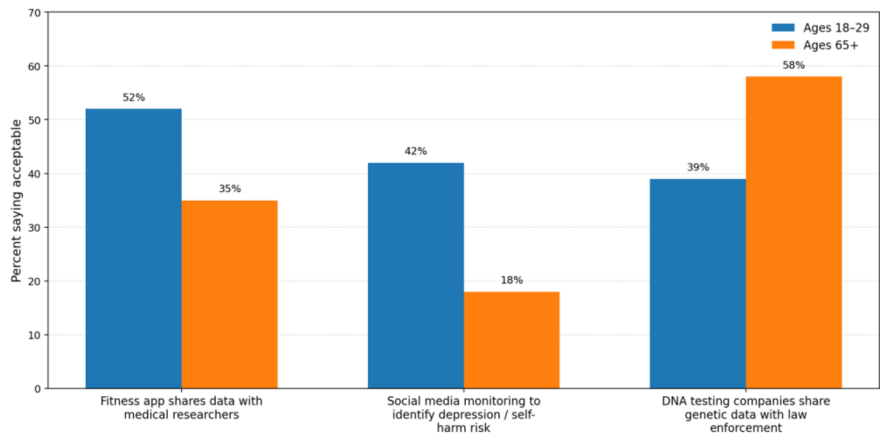


Fig 6. Willingness to disclose data for different purposes by age group. (Picture credit: original)

The figure 6 compares adults aged 18–29 and adults aged 65+ across selected data-use contexts, showing that younger adults are more willing to share data for health or well-being purposes, while older adults are more willing to share data for law-enforcement purposes. Data adapted from Pew Research Center [3].

6 Conclusion

Therefore, the traditional trade-off model fails to consider individuals’ real-world behaviors. Specifically, data intrusiveness plays an important role in shaping people’s willingness to trade privacy for security, since as the data collected becomes more sensitive and private, the probability that individuals are willing to disclose such information decreases greatly. Moreover, individuals’ willingness to give up privacy decreases over time as the immediate emergency fades, showing the effect of time decay. In addition, perceived legitimacy increases people’s willingness to give up privacy, showing that individuals’ trust increases the acceptance of surveillance measures. The study also shows that generational variations have an influence on privacy decisions, as younger individuals tend to emphasize privacy over security, and that older individuals are more likely to sacrifice privacy for security.

Overall, the results of this study show that people’s willingness to trade privacy for security is dynamic, context-dependent, and trust-related, rather than a fixed cost-benefit relationship. Thus, future research should move beyond the traditional trade-off model and take multiple factors into consideration.

References

1. Solove, D.J.: Nothing to Hide: The False Tradeoff Between Privacy and Security. Yale University Press, New Haven (2011)

2. Dinev, T., Hart, P.: An extended privacy calculus model for e-commerce transactions. *Information Systems Research* 17(1), 61–80 (2006). <https://doi.org/10.1287/isre.1060.0080>
3. Pew Research Center: Americans and privacy: Concerned, confused, and feeling a lack of control over their personal information (2019). <https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/>, last accessed 2026/04/25
4. Markos, E., Labrecque, L.I., Milne, G.R.: A new information lens: The self-concept and exchange context as a means to understand information sensitivity of anonymous and personal identifying information. *Journal of Interactive Marketing* 42, 46–62 (2018).
5. Pew Research Center: Ten years after 9/11: Public yields on privacy but marches on with liberty (2011). <https://www.pewresearch.org/politics/2011/09/02/ten-years-after-911-public-yields-on-privacy-but-marches-on-with-liberty/>, last accessed 2026/04/25
6. Pew Research Center: Americans feel the tensions between privacy and security concerns (2016). <https://www.pewresearch.org/short-reads/2016/02/19/americans-feel-the-tensions-between-privacy-and-security-concerns/>, last accessed 2026/04/25
7. Pew Research Center: More support for Justice Department than for Apple in dispute over unlocking iPhone (2016). <https://www.pewresearch.org/politics/2016/02/22/more-support-for-justice-department-than-for-apple-in-dispute-over-unlocking-iphone/>, last accessed 2026/04/25
8. Meng, X., Li, Y., He, Q.: Pathos or logos? How governance legitimacy perception influences individual privacy trade-offs during the COVID-19 pandemic. *Humanities and Social Sciences Communications* 11, Article 451 (2024). <https://doi.org/10.1057/s41599-024-03212-0>
9. Kehr, F., Kowatsch, T., Wentzel, D., Fleisch, E.: Blissfully ignorant: The effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal* 25(6), 607–635 (2015).
10. Pew Research Center: How Americans view data privacy (2023). <https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/>, last accessed 2026/04/25

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (<http://creativecommons.org/licenses/by-nc/4.0/>), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

