# A Balanced Scale: Convenience and Security within the Age of AI

## Andrew Nunez

## Fordham University

## New York,NY 10023

# Abstract

While the age of technology has continued to revolutionize the modern era, with it comes concern. Society has acclimated to the evolution of new technologies and integrated them within our daily lives as they continue to become more prevalent. However, as reliance on this technology has become more prevalent, so has the level of convenience it has demanded. Accessibility and convenience of data and internet connectivity have become incrementally more important in people's daily lives as reliance on them grows. This has emphasized the user experience and assurance of constant uptime and availability along with ease of use. Ultimately this has caused negligence in the space of cybersecurity regarding these devices, as data security and protection of privacy are sidelined in favor of catering to the front-end user experience. This raises alarming concerns surrounding user privacy, confidentiality, and data security amongst countless devices and applications. We must break down the causation, effects, and future should we continue down this path. Security must become a priority in the development stage in order for it to become increasingly standardized.

# Introduction

The complexity of hardware and software has only risen, and with IoT and smart devices becoming increasingly commonplace, it is once again brought to the forefront as to the protections in place for user information. Accessibility to these devices has remained paramount to consumers, as well as connectivity and simplicity. With this comes into question the safety and security measures being put in place to combat threat actors and malicious acts against users. This becomes increasingly concerning as dependence on these devices grows and the cyber landscape continues to veer more into smart homes and cities. This concern grows even further as AI models and LLMs(Large language models) take the spotlight and have become the focal point of tech evolution. AI has taken the world by storm, and tech companies seek to capitalize on the current sphere by deploying their models and integrating them within their already existing products. This then adds to growing concerns surrounding how far developers are willing to sacrifice data privacy and security in the name of simplicity and convenience.

What began with application and software security has evolved into concern regarding the security and safeguards in place within IoT devices and LLMs. It has become increasingly concerning as to the security within everyday IoT devices and potential data leakage or interception by malicious actors. The prioritization of fluid connectivity in the simplest manner possible with minimal overhead for proper security infrastructure. LLMs and generative AI models exacerbate this dilemma as they become further integrated with existing devices and software. The information inputted by the masses into these models and being collected from users all over the web is also at risk of falling into the wrong hands and potentially being utilized by foreign national actors (the DeepSeek model is based primarily within China).

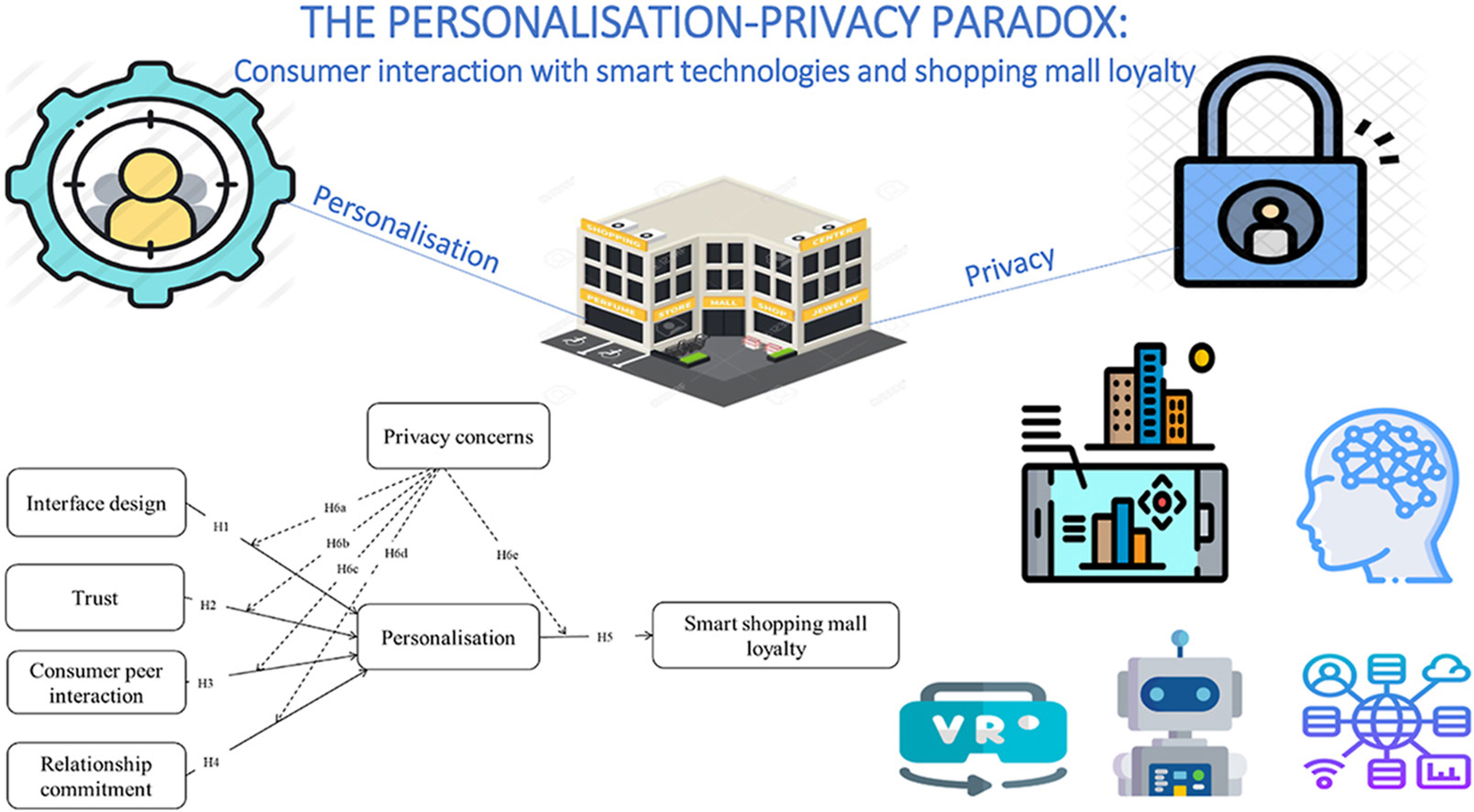
Security regulations and standards require participating organizations to comply and ensure standards are met to protect users against data compromise and threats. Despite this, however, to maintain profits from users, an emphasis is placed on ensuring constant uptime, connectivity, and convenience. This then provides space in most cases for the bare minimum of security within these products and activities. What this then evolves into is a social push where more convenient options become the preferred option rather than veering towards more secure options. If security is to become a priority within the modern landscape, it must then take a form suitable for the consumer base and sway social standings towards a more caring outlook for privacy and security rather than UI appeal.

# Social Pressure

Social influence has played a major role in the acceptance and normalization of various platforms, items, and staples within our everyday lives. Whether it is apparent or not, the majority of individuals lean more towards what is popularized within the culture, and that tends to be the most convenient and appealing option. In doing so, we propel applications, software, and hardware that, while simplistic in design and easy to utilize, are less secure and may potentially leave countless users at risk. This then begets a herd mentality towards these options and away from more secure and robust alternatives. Unencrypted messaging platforms and weaker alternatives are utilized due to their prominence in the public eye (i.e., WhatsApp, Google Messages, and Snapchat), where more secure options (Signal and Wicker) are less favored. In practice, most users will lean towards the option they view as being the "lesser hassle," to such an extent that some research cases even show that requiring even more extensive protections for a password will turn potential users away.

It can be argued that the social and peer pressure to conform to more popular options is what drives the populace to these platforms. Within surveys and interviews taken within the respective user bases, the main points of intrigue leaned toward ease of use, simplicity, and accessibility. A prominent example was the reliance on Google Maps despite the more secure and comparatively robust option of Maps. It seemingly boiled down to the overall prevalence of the Google-based application within social circles as well as the more simplified UI and approach towards GPS services that it provided in comparison to alternatives. What drives users towards alternative pressure is ultimately not just the UI and benefits of the platform but the stigma and reputation of the thing in question. X, formerly known as Twitter, remains a goliath within the online space despite numerous concerns for data privacy, scraping, and recent data leaks/attacks. While decentralized and security-driven alternatives like Mastodon and Blue Sky exist, they remain smaller players as X maintains its space on the social hierarchy as most online users congregate on what is the most prominent and accessible platform. Despite the risk it may pose to the privacy and security of their information, users continue to flock towards whatever is most popular rather than what is in their best interest.

A common theme in regard to the proper establishment of the mentality that is "security first" amongst users is a mentality that their data is already out there, so taking further precautions to protect it that may hinder their experience online is pointless. It not only feeds into the growing dilemma that will exacerbate the growing concern of data, personal information, and financial data being at further risk from threat actors and data leakage. Further research showcases that this is perpetuated via the media presence large-scale breaches demand, and many pinpoint the beginning of this thought process to the Equifax breach of 2017, which compromised an estimated 150 million people. This lack of concern for user data becomes a social issue that, if not properly treated, can snowball into frequent breaches and data theft of various magnitudes. With technology having become integral within everyday society, our constant connectivity, habitual usage of online services, and subconscious use of IoT and AI-based applications also begin to dull the concerns of the people. This constant usage begins to act as a dampener within the users as they become less concerned with protections and security as they assume their data is either a) not valuable enough to be targeted or has already been a part of a leak or breach and can be found online, so further protection is a hassle. A shift in philosophy towards security first is imperative in development to drive user focus towards these products that provide infrastructure to protect their data and information while simultaneously providing a simple manner of usage and unobtrusive methodology to bring in more users. Shifting social perspective begins with regulations and appealing to their desires for simplicity in the front end while providing a robust back-end protection system. By doing so, applications and devices can begin to establish parameters for user protections and eventually emphasize the importance of practicing cyber hygiene and protecting individual data and privacy. As we see, this breeds competition, which then breeds innovation within the space where already established large-scale organizations establish further parameters to maintain their user bases.



*Figure 1: The “Privacy paradox” in regards to users concerns against increased personalization[[1]](#footnote-0)*

At some point within this analysis, the concept of user privacy being within the hands of the user must be addressed. The evolution of the online experience has gone from that of a shared one to that of microcosms and tailor-made experiences. In doing so, we have seen the rise of cookies and data tracking to ensure each session is tailored towards its specific type of user. This provides personalized sessions and software that can be tailored specifically to their user and their habits. As can be imagined, this requires a stream of data from the user to ensure things are provided optimally. This adds concerns to security regarding what is being picked up and collected by these organizations. What this crafts is what would become known as the "Privacy Paradox," which emphasizes the push towards a more curated and personalized experience that, while driving social appeal, leaves users' privacy and confidentiality at risk. Despite this, these same individuals are more likely to conform or move towards a better service than prioritize their internet safety, despite any concerns they may hold regarding security.

# Legislature and Regulatory Practice

While tackling the ever-present scale of "convenience vs. security" at the social level for a peer-to-peer connection is important, it cannot be fully executed without addressing the laws and regulations put in place, and in some cases the lack thereof. Change begins with the enforcement of proper regulations and safeguards being put in place and enforced to ensure compliance is met by all institutions to push a more security-focused agenda. While convenience and accessibility are a priority, they can no longer overshadow growing concerns of data falling into the wrong hands and being used for nefarious purposes. In some cases, it can be argued that these changes for a more balanced approach are better for all parties involved. The EU's establishment of the General Data Protection Regulation provided a spotlight for a new data protection framework, which aimed to increase personal control over data. This highlighted a need for protection and consent for user data and began a larger-scale analysis of the absence of proper security measures in place for users.

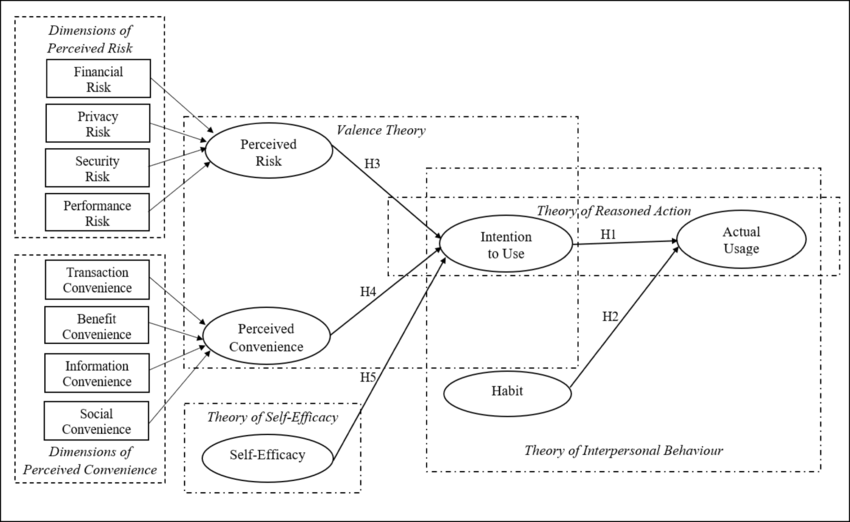
While this pushed for a prioritization of consumer security and data privacy, it brought to light how far individuals will push for security when they believe it impedes their experience. Many users argued in favor of better service and availability at the sacrifice of privacy, as convenience is paramount. It becomes abundantly clear that GDPR policy expansion is the future of cyber-first legislation but also that privacy and security can become more ingrained within the public sphere as the behavior can be socially constructed through peer connections and influence. In doing so, previous policies and future legislation will become more widely received, and users will begin to lean more towards options that ensure their security rather than whatever is most convenient despite detriment toheir well-being.

Without delving too deeply into the actual workings of the model itself and the influence it and others like it hold over the landscape, the question of deep confidentiality has been brought into question on numerous occasions. DeepSeek being a model primarily developed within China as well as being open source raises questions surrounding its data practices. With the model being under the jurisdiction of the Chinese government, it leaves current policies and legislation in a state of limbo regarding its stature and capabilities as well as the intentions behind the collected data. The nature of its novelty leaves it in a state where precedence is lacking in how to properly approach it, and due to its impressive capabilities, especially with regard to financial organizations and healthcare, it would hinder growth to outright place a ban on its usage.

Regulations and legislation within the cybersecurity landscape have improved steadily within the year as we bear witness to NIST- and SOX-based influence spread amongst other practices. Despite this, however, enforcement and implementation of said processes leave much to be desired. Organizations prioritize newer demographics seeking bells and whistles rather than robust security measures, which may impede their ability to access things instantaneously. By enforcing proper procedure implementation as well as requiring strict parameters surrounding security audits during the production phase, it is possible to provide a more robust back-end security infrastructure that does not impede the user experience and drive away the convenience afforded to users. In its stead, allow legislation such as GDPR-based concepts to be expanded upon, and along with the growing usage and normalization of security standards such as 2FA, passkeys, and other similar measures, perhaps security standards may also grow to become normalized within the industry and society.

# IoT Safeguards and Convenience

Regulations and legislation within the cybersecurity landscape have improved steadily within the year as we bear witness to NIST- and SOX-based influence spread amongst other practices. Despite this, however, enforcement and implementation of said processes leave much to be desired. Organizations prioritize newer demographics seeking bells and whistles rather than robust security measures, which may impede their ability to access things instantaneously. By enforcing proper procedure implementation as well as requiring strict parameters surrounding security audits during the production phase, it is possible to provide a more robust back-end security infrastructure that does not impede the user experience and drive away the convenience afforded to users. In its stead, allow legislation such as GDPR-based concepts to be expanded upon, and along with the growing usage and normalization of security standards such as 2FA, passkeys, and other similar measures, perhaps security standards may also grow to become normalized within the industry and society.



*Figure 2: Model showing perceived risk vs convenience model[[2]](#footnote-1)*

Security potential within these systems is essential as they become more and more complex and grow increasingly widespread. While seamless connectivity remains the main appeal as well as its automating capabilities, layered security structures continue to showcase the future of security as we move more towards smart cities and more interconnected ecosystems. Due to their limited computational and processing capabilities, applying a secure-by-design model and multilayered architecture can deter large-scale breaches and leaks in the long term while securing potential threat vectors within the greater network.

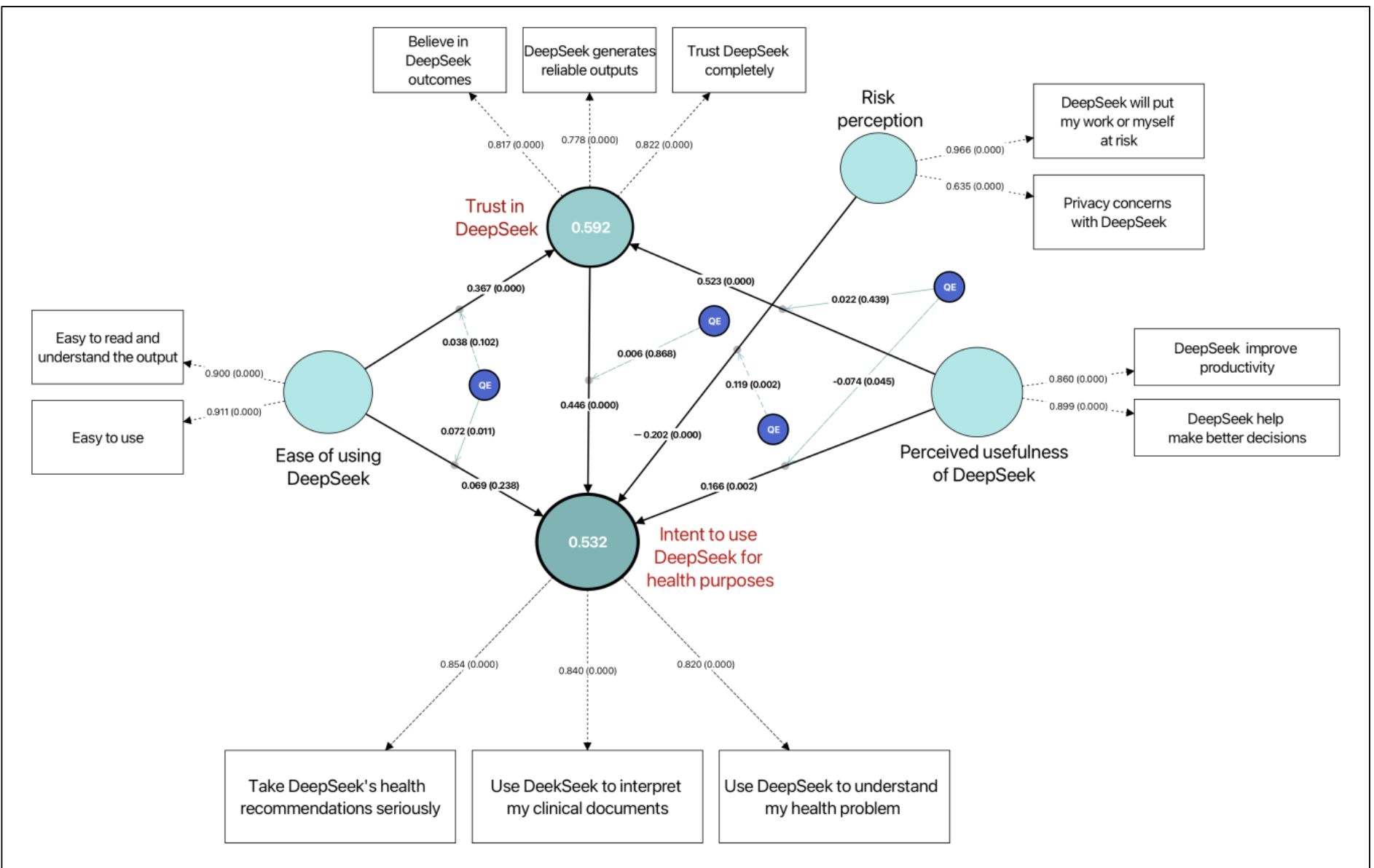
# The Era of AI

Like IoT before it, the latest marvel in innovation that is soon to be integrated into as many aspects of everyday life as possible is the rise of AI and large language models. Its relevance can not be understated and perpetuates a whole new level to the struggle between cybersecurity and user convenience. At their core, many of these models employ data-scraping methodologies, and many utilize the data inputted by users to further their learning model and continue to improve. At its core, it is seemingly harmless but once again raises flags about the protection of user data and removes further user ownership due to the nature of data scraping. We are already witnessing not just the competition of several model organization models, such as Gemini, GPT, Llama, and DeepSeek, to name a few, but also their integration into countless already existing interfaces. It raises questions surrounding the ethics of its data collection and what safeguards are in place to prevent user data inputted by these models from being subject to a potential breach or leak. With DeepSeek's explosive rise on the scene due to its low hardware overhead and its computational power on a budget, it also leaves curiosity as to not just the intentions of the Chinese-owned model but also the legality surrounding data protection by a foreign jurisdiction that stands in opposition to the West.

DeepSeek's intrigue begins with its accessibility, as it is capable of running on fewer resources than other models and has demonstrated capabilities of rather quick collection and learning processes. This acts as a lower barrier for entry into the space and allows for more mid- to low-level organizations to employ its usage at a smaller cost than something akin to GPT or Copilot. This has brought into question the consideration of security and what occurs in the backend, which allows for this low-cost efficiency to occur. Concerns arise when introducing its applicability into systems such as those of a healthcare organization. With large amounts of PII and PCI being prevalent along with the existence of industry regulations and practices such as HIPAA, concerns surrounding privacy within the DeepSeek model arose. The inability to properly trace the data within the model as well as the endpoint ultimately being within China-centric entities causes questions and concerns as to what this data may be used for as well as measures taken to safeguard it.

The competition between these major organizations in their models has stirred a frenzy to see which model can reign supreme over the rest. In doing so, compromises are made to ensure efficiency and drive up user numbers. Once again, security is pushed to the wayside and ultimately could prove disastrous in the long run. Implementing these models demands proper security infrastructure to prevent foreign threats from compromising these models and their data, which could pose a threat to the entire interface and be dangerous in the potential altering of its output. Mass harvesting of data leaves user sessions susceptible to compromise and potential data leakage, which, if unattended to and continuously implemented within existing software and hardware, could have wide-reaching consequences regarding existing infrastructure integrity and leave countless systems at risk to those seeking to utilize the collected information and queries for their purposes.

Transparency and trust lay the groundwork for proper AI implementation. The recency of their rise leaves time for proper examination and future formation of regulations to be implemented to protect endpoint users. Requiring limitations be put in place as to how long data may be retained as well as functioning protections against data scraping that require domain consent are a strong start in striking a balance between the ease of use and convenience of the systems while maintaining security and interoperability.



*Figure 3:Deepseek infrastructure and pathways of usage and reasoning[[3]](#footnote-2)*

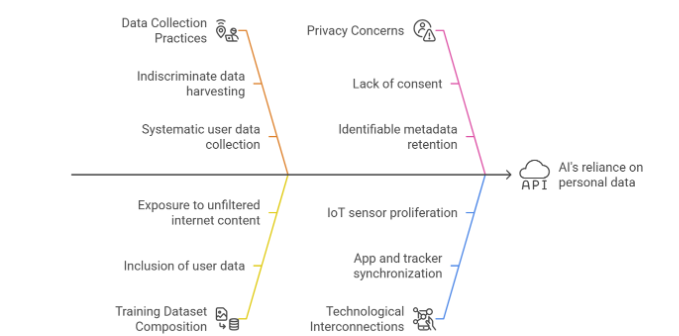
Major players within the AI race, like Gemini, GPT, Meta LLAMA, and DeepSeek, among others, are pushing the industry as much as possible to remain ahead of the competition. In doing so, they leverage all their resources towards the continued growth and development of their systems and models at the cost of user privacy and protection. With the AI frenzy being as new as it is, regulations and the like are yet to catch up, thus creating a void in the space that allows for more leeway in its capabilities of data usage and manipulation. The collection of data from data scraping and gathering via user queries and inputted information remains unimpeded for the most part, with loose security practices being the main defense against it and little potential to ensure these entities are not retaining sensitive user information to further grow their models' learning capabilities. This falls under the continued pretense perpetuated by these organizations that this allows the model to grow and learn and, in some cases, usually barred behind a premium model, allow for a more tailored and personalized experience for the user. By providing the user with a more tailored experience where the AI session utilized by them learns from their behaviors and approach in using it to where it becomes more appealing and easy to use. This elevates to a point where users begin inputting sensitive information or personally identifiable information into the system to automate certain tasks and production processes.

This normalization of sharing sensitive data and information with these models despite any awareness as to what it can be used for or done with on the opposite end once it has been collected. It is destructive to security integrity as well as further stripping away at the user's privacy levels for the sake of making things simpler and easier to do. Deterrence, such as the robot.txt protocol attempting to deter these LLMs and other AI models from mass data harvesting, tends to be bypassed and largely unenforceable due to the overall newness of the field and the questions surrounding data ownership online. With the lack of enforcement of data ownership and transparency regarding data harvesting and retention, users are left susceptible to large-scale data leaks should any used engine be compromised. This becomes increasingly concerning as it becomes increasingly integrated into existing platforms that are staples in the daily lives of countless individuals.

The on-demand simplicity and convenience of AI models has pushed for their inclusion into many already existing platforms. From browsers and already existing software, including background AI assistants, to integration with existing hardware like Apple Intelligence and Amazon's Alexa+,. With the pretext of simplifying and automating tasks and providing a smoother and easier user experience, many are willing to maximize the potential of these new concepts without considering how it may impede their overall privacy and hardware integrity. The lack of transparency on the back end of these models and the retention and collection of user data act as a major threat towards security. Lack of infrastructure and proper implementations of data deletion and ownership that would empower users more and add expiratory limits to how long data can be retained also are major causes for concern. Safeguards and expulsion of information within the line of PII, PCI, and similar confidential data that may be gathered by AI models must be put in place as they operate more and more within our daily lives. Ensuring that its usage remains surface level in its usage levels within our hardware would allow for its simplicity and convenient usage to remain in place while providing a layer of protection towards how much data it is able to collect and utilize. Proper education on cyber hygiene as well as privacy in using AI is a necessary step forward in the growing sea of AI dominance.

# Perception and AI in action

In regard to the influence that the convenient and easy use of modern technology and applications has had on society, it is seen as being in competition with other aspects in play. Essentially, features being provided and the experience of the user base are seen as being prioritized over other aspects such as the security of the service and backend. However, this is in the eyes of the average user, where it is viewed as one must sacrifice the other in order to exist functionally. In speaking with a small survey sample of working individuals between the ages of 25 and 55, a common trend was a focus on the features provided by their most used online services and applications, along with how easy it was to maneuver within them. While when asked to what level they value the security of their data within these programs and services, they tend to lean more towards those that are easier to access and popular amongst their social circles. One such example was the use of services like WhatsApp and X (formerly known as Twitter) over more potentially secure options such as Signal or Mastodon. Those who were aware of these alternatives pointed to the popularity of the former in regard to use cases and how it was “simpler” for them to remain in touch with things. Many note the importance of securing their data, but a trend I noticed was younger generations viewed it as relatively “pointless,” as they assume, with all the news regarding breaches and data shared between ad agencies, that their data is already available to anyone who really wants it. MFA has become increasingly popular within many applications and services to such a degree that people have come to view it as just another norm. This lends proof to the ability of conditioning people into accepting more secure options and potential by conditioning them over time to see it as just another part of their daily lives. Many cite an emphasis on security within their applications but are driven away by the lack of customizability within these more secure options. A lackluster feature set then becomes associated with these more secure options, thus creating a narrative amongst the people that these experiences are limited by the security implementations.

*Figure 4:AI Dependance on data and privacy risk[[4]](#footnote-3)*

Usage of AI models also remains in question as throughout the world usage has become increasingly commonplace. People remain suspicious of these models but remain complacent in the data they input into these models due to the narrative being pushed that “ their data is out there, so why bother?” AI's potential to siphon the information gathered from user queries remains in question as to whether it can be accessed via another user's session. In brief testing, it seems while ChatGPT remained more conspicuous in the data it would provide based on specific queries regarding individuals, Gemini and DeepSeek, on the other hand, were more open-ended. In a brief test from one device, I pushed queries into the GPT-4 model regarding a healthcare business under the pseudonym Orchid Healthcare, with specific mentions of a made-up employee going by the name Maya Daniels. When attempting to garner this data from another device and account, ChatGPT remained inconspicuous as to the specifics I had mentioned previously and even offered alternative public companies under a similar name. Gemini and Deepseek, while also not providing details such as the fake phone number and salary of the made-up employee, did offer increasingly more specific search query suggestions. This does lead to increasing intrigue in regard to the privacy of these models and their rampant usage within the business world. Countless employees have employed these LLMs and AI models in an effort to complete their tasks in a quick and efficient manner due to the ease of use surrounding the query-based systems they abide by. When speaking with risk-based department members within a large-scale law firm, they made a point of highlighting the dangers of employees inputting sensitive documents and information into things such as GPT, as this classified data could be parsed by these models and potentially made available despite its confidential nature.

# Future Outlook and Recommendations

When I initially began researching convenience and security in regard to their relationship over time through the rapid evolution of technology, the focus remained primarily on the concepts in which they clash. The further and more in-depth this search took me, the more the initial concept evolved as well. The reality that became clearer within my perspective is that it is not an issue where one must be prioritized over the other, but instead, the two coexist in a balance where there must exist cohesion between them to continue to improve upon themselves. With IoT becoming an everyday normality and AI having taken over the current spotlight, the importance of "Secure by Design" has never been more necessary. In the most basic sense, it begins with the production of proper security architecture in the development stage. These devices and software applications are not just commonplace in this day and age but form the very basis of many important factors in the current state of the world. Ranging from healthcare implementations to business infrastructure down to simple home networks and usage of smart devices, it can no longer be afforded to focus on one or the other but instead, provide a robust backend security architecture while enforcing security standards until they too become second nature and another part of everyday life.

At the most basic level, moving security more towards the limelight and balancing the scales of convenience access with proper defense and security measures begins at the personal level. It's been demonstrated across the board that the overall population does not entirely disregard the importance of proper security measures but instead seeks out the options that provide them the most accessibility and tailored experience. Providing simpler and easier-to-understand UI models as well as pushing more focus on the value of securing your data and privacy within the provided service will be a twofold approach. Bringing in a more common-themed service will serve as more appealing to the masses while also providing an essential message sharing the importance and benefits of proper security implementation. If successful, it will push competition to also alter their approach to ensure their user base doesn't dwindle. It can already be viewed in practice with the recent push towards privacy within the session by search engines like Safari and Firefox, thus taking advantage of the ongoing federal investigation of Google. It begins by bringing it to the attention of the population, subtly showcasing the appeal and importance of a more secure-by-design approach and its small footprint and minimal impedance of the overall experience compared to its benefits. With 2FA and passkeys becoming increasingly common, it bodes well for further pushes and approaches revolving around endeavors such as proper encoding procedures and tighter data transport processes and protections.

Security and convenience must exist in tandem to ensure a smooth user experience in which CIA is maintained without compromising on the overall service being provided but instead building upon it. NIST, SOX, HIPAA, GDP, and many other forms of legislation and regulatory practices are becoming industry standards and continue to see applicability and evolution as we bring about new and more impressive computational capabilities. But it cannot stop there; regulations must come to pass and build upon GDPR ideals in order to promote a stricter secure-by-design policy on all agencies within compliance before being able to push the product into the global market. Data privacy and security being afforded to all individuals to protect themselves in this day and age is paramount as we delve further into the unknown advancements that come with each passing day.

A lack of proper infrastructure surrounding maintaining data transparency as well as the removal and destruction of personal and confidential information has remained a concern within the public eye. Agencies that promote these deletion services are often overly convoluted and, in most cases, are not capable of providing an extensive end product. Providing sites with regulations to ensure that user data cannot be stored past a certain amount of time (effectively an "expiration date," so to speak) in which the user must be notified within the time period would allow for a greater range of user input. With the mass amounts of data harvesting and agencies dedicated to utilizing and selling user data, methods of removing this data and opting out of permanent data retention would be massively beneficial in the long term so long as agencies continue to build upon and strictly enforce these aforementioned concepts.

IoT prevention starts at the root of the dilemma. which is the intricacy of the process itself. All these devices are interconnected, and in doing so are fountains of data for the taking. Promoting a secure-by-design hardware model is the first step in ensuring data security without compromising the endpoint experience for users. By employing things such as EMIs (electromagnetic interfaces) that use conductive/magnetic materials to detect/absorb stray electromagnetic fields to prevent threat actors from seeking to harm via eavesdropping or taking advantage of data leakage from these devices. This process, similar to RFID preventative measures used within credit card protection, would provide a more secure communication network amongst devices while allowing the overall experience of utilizing the products to remain smooth and easily accessible to the user. Also, by leveraging the strength of modern-day cloud-based technologies as a form of key management system, as we see being slowly implemented within browser-based and iOS key escrows for user passkeys, it can ensure secure and efficient key distribution for its users. Furthering the potential of secure data transfer around the clock within the IoT data transfer and acquisition process by larger systems and other devices. Multi-layered structures of security levels, which combine the secure data storage and transmission capabilities of AES and the secure device authentication and key exchange processes of ECC, are the future of stable and secure IoT data acquisition. By providing a more complex infrastructure within these devices during development and leveraging advancements in existing technologies, not only can they be more secure without impedance in their ease of use and convenience, but also they can be expanded upon in the future, thus adding longevity and further safety measures in the long run.

AI has taken the globe by storm and shows no signs of slowing its rapid growth in the near future. Tech giants have done everything possible to stay ahead in this race between one another at the cost of those whose information is being gathered en masse to further the models' learning patterns and, in doing so, being left at risk of potential data theft or manipulation. Primarily, as it is a new threshold, it must be made understood to all who utilize this tool that it is just that, a tool. In utilizing it, despite the ease of use and infinite capabilities it can be used for, whatever data is inputted into the query system is used by the model and organization to push it further. Utilization of this technology to allow it to parse and process personal data and information, which is then gathered within its data banks, should be frowned upon. DeepSeek alone has proved its potency with its ability to run on less intensive hardware in comparison to its competition while yielding impressive results and capabilities. And with this comes an influx of users who are not considering the issues presented in sharing their information with a model primarily developed within China, which is out of the jurisdiction of our regulatory and legislative capabilities. Data being harvested and gathered by the DeepSeek model is within the parameters of Chinese legality, thus leaving users in the dark as to what their data could be used for. With this low overhead comes risk at the cost of compromising proper security and data retention methods in favor of raw computational power. AI continues to grow, but with it must come safety measures in the shape of data transparency compliance and improved moderation of its processing capabilities and log retention. Its widespread use shows the capabilities of a simple-to-use platform in the hands of the masses, but restrictions must be placed on the potential it has of inflicting potential harm to others by providing safety measures to the user base in how it can be utilized and the extent to which it can continue to harvest information indiscriminately without any reins.

1. Final Thoughts

Security and convenience are not opposing factions but instead two ends of a scale that may not be perfectly balanced, but we must ensure one does not grossly outweigh the other. Security has taken a backseat in the rapid evolution of technology in the modern age but must be brought up to speed in a time when users are more susceptible to risk than ever before. Every step towards balancing this scale requires thought and care to not overstep and harm the end experience but instead form a new status quo to be followed. By practicing and implementing concepts and policies promoting a more secure and privacy-centric philosophy to the benefit of the average user, the establishment of something that can be expanded upon even further into the future becomes increasingly important. AI tools and LLMs are here to stay and must be utilized to push the boundaries of what we believe to be possible but must also be approached with a similar philosophy surrounding the value of data security and privacy while maintaining the accessibility and convenience that people have come to expect within the modern age.

##### References

1. Tarale, Himanshu & Renukdas, Mr. (2025). The Trade-off Between Security and Convenience: Finding The Sweet Spot!!!.<https://www.researchgate.net/publication/388679671_The_Trade-off_Between_Security_and_Convenience_Finding_The_Sweet_Spot>
2. Dr. A. Shaji George. (2025). AI Supremacy at the Price of Privacy: Examining the Tech Giants’ Race for Data Dominance. *Partners Universal Innovative Research Publication*, *3*(1), 26–43. https://doi.org/10.5281/zenodo.14909763
3. Evaluating the Performance of the DeepSeek Model in Confidential Computing Environment},author={Ben Dong and Qian Wang},
4. Temsah, Abdulrahman, et al. "DeepSeek in Healthcare: Revealing Opportunities and Steering Challenges of a New Open-Source Artificial Intelligence Frontier." *Cureus*, vol. 17, no. 2, 2025, e79221.
5. Krause, David, DeepSeek and FinTech: The Democratization of AI and Its Global Implications (January 29, 2025). Available at SSRN:<https://ssrn.com/abstract=5116322> or [http://dx.doi.org/10.2139/ssrn.5116322](https://dx.doi.org/10.2139/ssrn.5116322)
6. Temsah, Abdulrahman, et al. *The Human Cost of DeepSeek.* Rivista AI, Mar. 2025,[www.rivista.ai/wp-content/uploads/2025/03/THE-HUMAN-COST-OF-DEEPSEEK.pdf](http://www.rivista.ai/wp-content/uploads/2025/03/THE-HUMAN-COST-OF-DEEPSEEK.pdf).
7. Choudhury, Avishek, et al. "User Intent to Use DeepSeek for Healthcare Purposes and Their Trust in the Large Language Model: Multinational Survey Study." *arXiv*, 25 Feb. 2025, [arxiv.org/abs/2502.17487](http://arxiv.org/abs/2502.17487).
8. M. Gupta, C. Akiri, K. Aryal, E. Parker and L. Praharaj, "From ChatGPT to ThreatGPT: Impact of Generative AI in Cybersecurity and Privacy,"
9. Oseni, Ayodeji, et al. "Security and Privacy for Artificial Intelligence: Opportunities and Challenges." *arXiv*, 9 Feb. 2021, arxiv.org/abs/2102.04661.​
10. Tucker, Catherine. "17. Privacy, Algorithms, and Artificial Intelligence". *The Economics of Artificial Intelligence: An Agenda*, edited by Ajay Agrawal, Joshua Gans and Avi Goldfarb, Chicago: University of Chicago Press, 2019, pp. 423-438. <https://doi.org/10.7208/9780226613475-019>
11. S. Dilmaghani, M. R. Brust, G. Danoy, N. Cassagnes, J. Pecero and P. Bouvry, "Privacy and Security of Big Data in AI Systems: A Research and Standards Perspective," 2019 IEEE International Conference on Big Data (Big Data), Los Angeles, CA, USA, 2019, pp. 5737-5743, doi: 10.1109/BigData47090.2019.9006283. keywords: {Artificial intelligence;Big Data;Data privacy;Security;Data models;IEC Standards},
12. [Carmody, J.](https://www.emerald.com/insight/search?q=Jillian%20Carmody), [Shringarpure, S.](https://www.emerald.com/insight/search?q=Samir%20Shringarpure) and [Van de Venter, G.](https://www.emerald.com/insight/search?q=Gerhard%20Van%20de%20Venter) (2021), "AI and privacy concerns: a smart meter case study", [*Journal of Information, Communication and Ethics in Society*](https://www.emerald.com/insight/publication/issn/1477-996X), Vol. 19 No. 4, pp. 492-505. <https://doi.org/10.1108/JICES-04-2021-0042>
13. Williamson, Steven M., and Victor Prybutok. 2024. "Balancing Privacy and Progress: A Review of Privacy Challenges, Systemic Oversight, and Patient Perceptions in AI-Driven Healthcare" Applied Sciences 14, no. 2: 675. https://doi.org/10.3390/app14020675
14. Pal, A., Herath, T., De’, R. et al. Is the Convenience Worth the Risk? An Investigation of Mobile Payment Usage. Inf Syst Front 23, 941–961 (2021). https://doi.org/10.1007/s10796-020-10070-z
15. Alessandro Acquisti et al. ,Privacy and human behavior in the age of information.Science 347,509-514(2015).DOI:[10.1126/science.aaa1465](https://doi.org/10.1126/science.aaa1465)
16. The personalisation-privacy paradox: Consumer interaction with smart shopping malls. *Computers in Human Behavior*, <https://www.sciencedirect.com/science/article/pii/S0747563221002995>
17. The role of security notices and online consumer behaviour. *Journal of Experimental Social Psychology*, <https://doi.org/10.1016/j.jesp.2015.03.002>​
18. Zhang, W., Lei, X., Liu, Z., Wang, N., Long, Z., Yang, P., Zhao, J., Hua, M., Ma, C., Wang, K., & Lian, S. (2025). *Safety Evaluation of DeepSeek Models in Chinese Contexts*. arXiv. <https://arxiv.org/abs/2502.11137>
19. Nisreen Ameen, Sameer Hosany, Justin Paul,The personalisation-privacy paradox: Consumer interaction with smart technologies and shopping mall loyalty,<https://doi.org/10.1016/j.chb.2021.106976>.
20. Abdullah, T. A. A., Ali, W., Malebary, S., & Abdullah, A. A. A. (2019). A review of cyber security challenges, attacks and solutions for Internet of Things based smart home. *International Journal of Computer Science and Network Security, 19*(9), 139–150.
21. Hu, T., Wang, K. Y., Chih, W., & Yang, X. H. (2018). Trade off Cybersecurity Concerns for Co-Created Value. *Journal of Computer Information Systems*, *60*(5), 468–483. <https://doi.org/10.1080/08874417.2018.1538708>
22. Abdullah, A. A. A. (2019). *A review of cyber security challenges, attacks and solutions for Internet of Things based smart home* (Doctoral dissertation, Liberty University). Digital Commons @ Liberty University. <https://digitalcommons.liberty.edu/doctoral/4801/>​
23. Wong, G. C. (2023). *Cognitive machine individualism in a symbiotic cybersecurity policy framework for the preservation of Internet of Things integrity: A quantitative study* (Doctoral dissertation, Liberty University). Liberty University.
24. Shen, C.-C., & Chiou, J.-S. (2010). The impact of perceived ease of use on Internet service adoption: The moderating effects of temporal distance and perceived risk. *Computers in Human Behavior, 26*(1), 42–50. <https://doi.org/10.1016/j.chb.2009.07.003>
25. Taking AI Personally: How the E.U. Must Learn to Balance the Interests of Personal Data Privacy & Artificial Intelligence [Humerick, Matthew](https://heinonline.org/HOL/AuthorProfile?action=edit&search_name=%20Humerick,%20Matthew&collection=journals)

---------------------- \*\*\*\*\*\*\*\*\*\*\*---------------------

1. Nisreen Ameen, Sameer Hosany, Justin Paul,The personalisation-privacy paradox: Consumer interaction with smart technologies and shopping mall loyalty,<https://doi.org/10.1016/j.chb.2021.106976>. [↑](#footnote-ref-0)
2. Pal, A., Herath, T., De’, R. et al. Is the Convenience Worth the Risk? An Investigation of Mobile Payment Usage. Inf Syst Front 23, 941–961 (2021). https://doi.org/10.1007/s10796-020-10070-z [↑](#footnote-ref-1)
3. Choudhury, Avishek, et al. "User Intent to Use DeepSeek for Healthcare Purposes and Their Trust in the Large Language Model: Multinational Survey Study." *arXiv*, 25 Feb. 2025, [arxiv.org/abs/2502.17487](http://arxiv.org/abs/2502.17487). [↑](#footnote-ref-2)
4. Temsah A, Alhasan K, Altamimi I, Jamal A, Al-Eyadhy A, Malki KH, Temsah MH. DeepSeek in Healthcare: Revealing Opportunities and Steering Challenges of a New Open-Source Artificial Intelligence Frontier. Cureus. 2025 Feb 18;17(2):e79221. doi: 10.7759/cureus.79221. PMID: 39974299; PMCID: PMC11836063. [↑](#footnote-ref-3)