

Beyond the Platform: Immutable Portability and the Governance of Persistent Personal AI Profiles

Submitted 17 September 2026, Revised 30 September 2026, Accepted 30 September 2026

KennaL.Young¹, Maurice McBride^{2,3*}

¹3 Fold Ventures, Florida, United States

²McBride Business Solutions, Columbia, United States

³Healthcare Cybersecurity Program, Department of Healthcare Technology,
Capitol Technology University, Laurel, United States

Corresponding Email: *mmcbride@captechu.edu

Abstract

Continuity through AI memory is changing the nature of artificial intelligence from session-based to more personalized. Current portability frameworks provide for the ability to access some data records, but not for the evolving universe of information comprising context, preferences, inferences, relationships, instruction, and provenance that makes continuity possible. In this Article, the universe of information making continuity possible is termed the Persistent Personal AI Profile (PPAIP), and Immutable Portability is proposed as a governing principle. Immutable Portability is made up of two components: the right and ability to access, retain, and transfer PPAIPs in functional format, and the limitation of post-termination beneficial use without an independent legitimate basis. This Article sets forth the idea of Immutable Portability in the context of existing European and U.S. frameworks governing portability and artificial intelligence, current platform export processes, research into the concept of portable AI memory, and personal AI sovereignty. The Article concludes that any such governance would require standards, supervision, revision capacity, and accountability, and deal with lifecycle issues of dormancy, incapacity, death, succession, destruction, and economic transfer.

Keywords: Artificial Intelligence, Persistent Personal AI Profile, Immutable Portability, Data Portability, Interoperability

INTRODUCTION

Personalization is one of the features of artificial intelligence that will become stronger and stronger. Thanks to persistent memory, artificial intelligence can remember previous sessions and utilize the stored data to adjust further communications. As this feature becomes better, the utility of a communication with AI will be defined by not one model reply, but by context gained during the whole period.

This context can include much more than just the history of the conversation. It may include user-stated facts, preferences, goals, relationships, instructions, project context, behavioral patterns, inferred characteristics, prior decisions, corrections, and system-generated summaries. A user may therefore develop a substantial individualized layer of intelligence that is practically valuable even though it is distributed across technical forms and may not correspond to a single file or database.

Portable memory is already an active technical and policy problem. Stanford-led work has proposed portable and persistent personal memory through a unified human-context layer

(Pentland et al., 2026), while the Portable AI Memory specification proposes a vendor-neutral format for exchanging memory objects with provenance, lifecycle, confidence, and integrity metadata (Gines, 2026). Recent work on personal AI sovereignty likewise argues for user-controlled longitudinal context rather than continued dependence on platform-centered extraction (Hothi, 2026). Stanford's work reaches beyond simple file portability to standards, lifecycle governance, accountability, purpose limitation, and user-controlled access. Those surrounding ideas are therefore not claimed here as new. The narrower contribution developed in this article is the combined principle of a non-revocable retrieval, retention, and transfer entitlement together with a restriction on the former provider's post-termination beneficial use.

The central contribution of this article is more specific and deliberately more forceful. It defines the Persistent Personal AI Profile (PPAIP) as a distinct governance object and proposes Immutable Portability as the principle that should govern a person's ability to leave an AI platform. Immutable Portability requires that the individual's practical ability to access, keep, and move his PPAIP be permanent and irrevocable. A service provider might terminate service, suspend an account, or end a business relationship, but should not be able to nullify the individual's inherent ability to take the profile. The second part of this principle also includes a complementary proposition: once the relationship ends, the previous provider should not continue using the person's PPAIP for his own benefit solely because he still technically owns some underlying data without a further valid reason for doing so.

The difference is important, since regular portability could be achieved easily by simply providing the user with a huge set of data that cannot be interpreted properly in another system. Having a copy does not address the issue of what information is retained, mined, inferred from, or used commercially after termination.

The governance issue does not end with a change of providers by an active user. A PPAIP can become inactive; its owner may become incapacitated; or the owner may die, leaving behind a profile containing years' worth of personal and third-party information. The mature governance regime, therefore, must deal not only with transfer but with lifecycle management: succession, archival storage, limited retention, destruction, and even the potential that inactive PPAIPs may become valuable analytically as technology advances.

This paper is normative in nature. It does not make the argument that current law already recognizes an entire PPAIP to be the property of the user, that all profile components are capable of being transferred, or that current laws create the rights proposed in this article. Instead, the article highlights an emerging governance object, analyzes the available legal and technical infrastructure, and makes a case for a governing principle to guide the future.

DISCUSSION

From AI Memory to the Persistent Personal AI Profile

Technical memory and a Persistent Personal AI Profile are two different terms that may sometimes overlap. For instance, the Portable AI Memory specification describes exchangeable memory objects and their metadata (Gines, 2026). It is important infrastructure indeed, but the governance object proposed in this article goes beyond that particular memory record.

In the current context, the Persistent Personal AI Profile is defined as the constantly evolving collection of data, context, preferences, characteristics, relationships, instructions, interactions, and other attributes that allows an AI system to achieve individualized continuity in its activities.

This definition is purposefully functional and agnostic towards architecture specifics. It does not imply the need to store the profile in a single database, in a single device or cloud of a certain provider. Its focus is on the individualized representation which will allow achieving continuity in the future. Thus, the issue of data storage becomes less critical in terms of governance than preserving enough of this individualized representation in case of change in custodians or providers.

An unrefined chat history may be valuable but fail this test. Chat logs do not always differentiate between information that is current and outdated, assertions and inferences of the system, stable preferences and one-time instructions, or between highly certain facts and less certain interpretations. The system receiving the chat history may in fact be able to read it without being able to recreate the continuity of the original relationship.

Existing Portability Regimes and the Persistent AI Profile Gap

1. Existing Legal Foundations

The notion of data portability is certainly not novel from a legal standpoint. Academic work on GDPR has focused on portability as a means to enable user control and interoperability (De Hert et al., 2018). GDPR Article 20 establishes a right to receive personal data provided to the controller in a structured, commonly used, and machine-readable format, and to transfer them to another controller without hindrance, provided certain conditions are met (European Parliament & Council of the European Union, 2016). The EU Data Act addresses the issues of switching, interoperability, and obstacles to transferring between different data processing services (European Parliament & Council of the European Union, 2023).

These legislative efforts certainly offer some useful precedent, yet they are difficult to apply to PPAIP. An advanced profile might include information that was provided by the user, information inferred about the user, provider-generated summaries, provenance relations, third-party information, as well as technical representations that cannot be easily categorized under the rubric of 'data provided'. Even more importantly, existing portability rights do not always guarantee that the semantic and functional integrity of an individualized AI relation is preserved.

2. AI Governance Does Not Yet Resolve Profile Portability

The EU Artificial Intelligence Act brings about a layer of AI governance, which entails obligations concerning data governance, transparency, risk management, human oversight, and privacy of personal data in certain contexts (European Parliament & Council of the European Union, 2024). The Artificial Intelligence Act, however, fails to provide a system for cross-platform portability of the personal AI profile. This is an important gap because although a jurisdiction may have a high level of development of its data protection rights and an AI act, the issue of the governance of the personal AI profile is only partly solved.

The very gap is revealing because while there are regimes addressing the issues related to adjacent categories—personal data, consumer rights, AI systems, competition, security, and platform switching—they do not address the issue of personal AI profile continuity, custody, reuse after termination, succession, destruction, and transfer. One possible explanation may be that the object of regulation has not been sufficiently defined.

3. The Fragmented U.S. Portability Landscape

A gap exists in the United States that is similar to the European gap. The Federal Trade Commission has reviewed data portability in terms of consumer control and competition, as well as concerns of secure transfer, third-party information, identity verification, standards, interoperability, and implementation (Federal Trade Commission, 2020). A 2019 report from the United States Government Accountability Office made recommendations for comprehensive federal Internet privacy legislation, with its current status on that recommendation being that as of February 2026, no such legislation has been enacted (U.S. Government Accountability Office, 2019).

The correct assertion to make, therefore, is that there does not exist a comprehensive federal framework for data portability in the United States. Such portability rights do exist under certain frameworks in state laws and sector-specific frameworks, but the gap lies in the absence of a comprehensive federal framework for portability and other consumer-control

rights in the context of persistent AI personalization (U.S. Government Accountability Office, 2019).

4. Current Platform Practice: Export Is Not Profile Portability

Current consumer AI services illustrate the distinction. OpenAI permits eligible ChatGPT users to export chat history and other account data and separately provides account deletion procedures (OpenAI, n.d.). Google permits users to export Gemini Apps data through Google Takeout and explicitly notes that downloading the data does not itself delete it from Google's servers (Google, n.d.). Microsoft allows users to export or delete Copilot activity history through its privacy dashboard (Microsoft, n.d.). Perplexity provides account-deletion mechanisms that remove profile details, preferences, settings, search history, sessions, and shared content within its stated deletion process (Perplexity, 2026).

These are important ways for users to exercise control, but the public documentation of these mechanisms is largely limited to levels of chats, history of activities, account details, settings, or deletions. These mechanisms do not, in their documentation, indicate how these features may be used to form a common cross-provider representation of the complete personalized context that is defined in this paper as the PPAIP. It is thus possible for the user to have many exported records and still not have a common means for recreating the personalized context somewhere else.

5. Personal Data Stores and Emerging Sovereignty Concepts

Personal data stores represent another architectural tradition that is designed to empower individuals with respect to their own personal information (Fallatah et al., 2023). Similarly, the work from Stanford concerning portable memory is based on the concept of user-controlled context layer that persists across different AI services and also includes the notion of standards, lifecycle governance, accountability, purpose limitation, and controlled sharing (Pentland et al., 2026). The recent paper from Hothi on personal AI sovereignty expands the argumentation to user-controlled personal AI environments and longitudinal data (Hothi, 2026).

The point here is not to state that the notions of portability, sovereignty, personal data stores, standards, lifecycle governance, accountability, or portable AI memory are novel. The contribution here is to link all these concepts to a more concrete governance principle that is related to the individual's capability to retrieve, retain, and transfer the PPAIP that cannot be revoked after the termination of the relationship between the user and the departing provider.

Immutable Portability

Immutable Portability is a dual concept. On one hand, an individual should have the non-revocable right and capability to retrieve, retain and transfer a PPAIP. This means that the term immutable refers to portability, not to what is contained in the profile itself. The profile must continually change along with the individual, his or her relationship and the technological background.

Termination of service, suspension of access, banning of a person, cessation of business, price increase or other changes in contractual relations are not reasons for deprivation of an individual's capability to transfer his or her personal data. Controls on security and identity and lawful restrictions may affect the timing or conditions of transfer, but not the capability to do so.

On the other hand, portability should deal with the post-departure period as well. A platform can satisfy minimal export obligations by providing copies of the data but continuing mining and commercial exploitation of the individualized profile. In Immutable Portability, we deny the idea that possession equals an unlimited right of exploitation. Beneficial use by the former provider requires its own ground after termination.

Therefore, the term Immutable Portability refers to the lasting and irrevocable right and ability of an individual to access, keep, and transport their Persistent Personal AI Profile in a form that is usable, independent of whether there is continuation, cancellation, suspension, payment, or any other state of the individual's association with a given platform, along with protection against post-association exploitative use of that profile by the former service provider unless there is a separate legitimate reason for such use.

The use of the phrase 'separate legitimate reason' is deliberately conservative. Legal requirements may compel retention of data for purposes of litigation, fraud prevention, audits, or other reasons. Retention doesn't have to mean exploitation of that data in some other way.

Counterarguments and Boundary Conditions

1. Provider-Created Representations May Not Be Wholly User-Owned

The strongest counterargument is that the PPAIP may include content created by the service provider and not necessarily contributed by the individual. Such elements may have claims to trade secrets, copyright, contract, or security issues.

Immutable Portability need not reveal all proprietary internals. It only needs to provide a portable version of the content sufficient for preserving user-specific meaning and continuity without having to expose the proprietary internal implementation.

2. Third-Party Information Complicates Exclusivity

Personal data contained within a PPAI may include details relating to spouses, children, coworkers, clients, or other third parties. It would be extremely challenging to make an absolute claim that all of the content of the profile is owned by the user alone. The portability and succession laws must not come into conflict with proper respect for the privacy, confidentiality, and intellectual property rights of the third parties. The notion must be taken to mean a right to a persistent user profile, subject to proper respect for any conflicting rights.

3. Security Controls May Delay but Should Not Destroy Portability

In the case of a compromised account, the problem becomes clear in that exporting the account immediately to the attacker could do much damage. The provider needs to have authentication, anomaly detection, recovery and transfer protection mechanisms in place. These would be consistent with Immutable Portability if they protect the rightful owner and can be reviewed.

4. Functional Continuity Cannot Mean Identical Behavior

There is no interoperability standard that can ensure that two AI systems would act in exactly the same manner. Models are different from each other in many aspects including architecture, security measures, abilities, window of context, and behavior. Thus, functional portability must be formulated more conservatively; that is, the recipient system must be capable of reading the standardized user-specific data without unnecessary loss of meaning.

Standards, Supervision, Revision, and Accountability

A portability right without interoperability standards risks becoming nominal rather than functional. Providers do not need to use the same models, databases, programming languages, or storage architectures, but they need a common exchange contract if a PPAIP is to move meaningfully between systems. The Portable AI Memory specification demonstrates that structured exchange with provenance, identifiers, hashes, temporal metadata, confidence, and lifecycle information is technically plausible (Gines, 2026).

A mature PPAIP standard would likely require at least three levels of interoperability. Syntactic interoperability means that a receiving system can parse the package. Semantic interoperability means that it can understand what the fields and relationships mean. Functional interoperability means that enough individualized context survives transfer for the receiving system to use the profile meaningfully without requiring the person to rebuild years of context from the beginning.

The standard would also need identity assurance, provenance, versioning, conflict resolution, tamper evidence, extensibility, security labels, temporal validity, and rules distinguishing explicit user statements from system-generated inferences. It should address safe import and export, malicious profile contamination, unauthorized duplication, and the treatment of provider-proprietary elements.

Standardization is not enough. Four functions are necessary for governance: standards, supervision, revision authority, and accountability. Standards outline the minimal standards expected. Supervision verifies that providers comply with the standards set. Revision authority ensures that the structure stays current in light of evolving AI architecture, memories, threats, and business models. Accountability produces consequences where commercial interests align with lock-in, incompatible proprietary solutions, and exploitative practices rather than user-centered interoperability.

The organizational home does not have to be predetermined. It can be an already established standards development organization, a regulator, a multistakeholder association, or even a newly formed organization. All that matters is functional capacity, with recognized authority for maintaining the standard and processes for verifying compliance with it. Certification, procurement requirements, auditing powers, contractual arrangements, regulatory endorsement, consumer remedies, penalties are just a few possibilities for further research.

The objective of the policy should be to make it more rewarding to conform than to defect. A rule that providers may violate at will when doing so is profitable cannot be called a rule.

Custody Without Captivity

Immutable Portability should be architecture agnostic. Custodian custody has valid arguments for its strengths in terms of advanced storage, authentication, redundancy, synchronization, availability, and security capabilities. User autonomy, therefore, does not necessitate that every user have a hosted profile on his local device.

The question of governance is one of determining which aspects are always true regardless of who is the custodian. In any case, the individual should be able to have the practical capability of accessing the profile, changing his custodian, hosting it elsewhere independently, and transferring the profile later. Portability should not mean the requirement of having a receiving platform at the time of departure from the old platform.

A user departing from Platform A may temporarily store the standardized profile in cloud-based storage, local storage, personal storage, vaulted storage, or any other custodial

storage. The decision of having redundancies of backup and the risk of independent custody should be up to the individual. It should not be necessary for former-providers to retain a copy simply because of the user's decision of self-custody.

Retention, Relinquishment, and Post-Termination Use

"Portability raises an issue that most export discussions do not address sufficiently well: what happens to the copy of the provider after the consumer leaves?" "An absolute deletion rule may run counter to any obligation the provider has to keep certain records legally." "A proper framework must take account of at least three conditions: active holding and use within the business relationship; legal retention with a defined purpose after its end; and value extraction for profiling, training, marketing, commercialization, research, or other value-generating activity."

It is an important principle for Immutable Portability. If the former provider continues to extract value from an individual-specific profile even after the individual has departed, portability would create a copy that transfers without transferring control. Legal retention should be purpose-bound and, where appropriate, segregated from business purposes.

This essay does not assume that present intellectual property law automatically renders a whole PPAIP copyrightable property or entitles the individual to a royalty. The profile may consist of legally distinct parts. The moral claim here is more limited: continued exploitation after the business relationship should not be presumed simply by virtue of the former lawful custody of the provider.

Lifecycle Governance: Dormancy, Incapacity, Death, and Economic Transfer

The notion of portability rights extends past active account usage into a lifecycle. There is some existing legal framework in relation to digital asset law which allows for the right of fiduciary access following incapacity and/or death (Uniform Law Commission, 2015), but a PPAIP may be different from a regular online account in the sense that it could be made up of user-generated content, inferences by the system, social maps of the user, external content, and the aggregate of representations of the individual's decision-making and preferences.

One useful way of conceptualizing the lifecycle is creation, active usage, evolution, transfer, dormancy, incapacity, death, and then succession, custody, or deletion. These different transitions would raise different issues. Can a user appoint someone who would have the right to retrieve or retain the profile in the event of incapacity? Does a power of attorney grant transfer rights? Can the individual mandate destruction upon death? What would happen if there is no successor?

The prospect of indefinite archiving creates yet another issue. Dormant or dead profiles may become more valuable as future analysis tools become more powerful. The information contained in the profile may have historical significance, proprietary information, intellectual property, evidence, family records, or any other potential value that was unknown at the time of its creation. This will create a conflict between the economic interest in keeping and mining a profile, on the one hand, and a person's privacy, destruction, and succession interests, on the other hand.

The question of divisibility and transferability of economic rights in PPAIPs may also become an issue in future governance. A person may transfer control over the profile but retain intellectual property rights, grant access for analysis without granting permission to exploit, authorize postmortem research but prohibit reconstruction, or permit the estate to benefit from future value through royalties or other reservation of rights. This example is similar to the notion of a bundle of rights rather than the sale of some indivisible asset.

Such a possibility of transfer also poses questions that are not answered by the current portability framework. Can a living individual sell or license their PPAIP? Can the decedent permit the transfer of access to the estate or the heirs? Are there any regulated markets for archival profiles? What survives transfer of the profile after death? What rights of the third parties or providers restrict such transfers? These questions are not answered by this article either. But their importance lies in the fact that the recognition of the PPAIP as an object of governance raises a new set of lifecycle and economic questions.

Interdisciplinary Research Agenda and Limitations

1. Research Agenda

It is not the intent of this paper to make the argument that one discipline can address all the questions posed by Persistent Personal AI Profiles. The value of this paper is to show how issues that are currently examined independently become interrelated in light of the full lifecycle of persistent AI personalization.

Legal scholars will want to explore the nature of the authorship of profile elements, termination rights, authorized retention, secondary use, licensing, succession, economic transfer, and the connections between profile management and intellectual property, privacy, contracts, and personality law. Standards and engineering groups will want to look at canonical schematics, semantic interoperability, binding of identity, cryptographic integrity, provenance, version control, safe transfer, deletion validation, and testing against standards. Cyber security experts will want to look at memory tampering, profile substitution,

unauthorized duplication, malicious imports, cross profile pollution, compromised transfer, and custodial attack surfaces.

2. Limitations

The article is theoretical and normative rather than empirical in nature. The article's analysis is based on existing literature and primary sources, but the state of the existing landscape of AI-memory and platforms partly depends on newer source material and documentation provided by the providers, technical specifications of these new systems, and very recent working papers which have yet to be peer-reviewed. It is possible that there may also be rapid changes in the abilities of the products and their retention practices. For that reason, the article illustrates its analysis using the examples of currently available platforms.

Implications for Cybersecurity Leadership

The key to the cybersecurity-leadership challenge is timing. Anticipatory governance involves the ability to take action in response to the emergence of new technology while still allowing meaningful intervention. Guston's definition focuses on foresight, engagement, and integration before the trajectory becomes too hard to change (Guston, 2014). The OECD framework for 2024 similarly contends that emerging and converging technologies require foresight-oriented governance based on values, strategic intelligence, stakeholder engagement, agile and adaptive regulation, and international cooperation in setting norms and standards (OECD, 2024).

Persistently tracking personal AI profiles is appropriate from this perspective because decisions may have to be taken before an issue becomes a cybersecurity problem. Once organizations and people develop years' worth of information that is not portable into other systems, the costs of moving away will increase.

This duty is also aligned with evolving cyber governance leadership role. An analysis of 250 CISO job ads in 27 countries reveals that the role goes beyond technology operation, and includes risks, regulations, standards, management, and executive-level responsibilities (Ramezan, 2025). The literature on CISO studies points to executive legitimacy, accountability, business realities, human element, and governance as central issues (Sahin & Vance, 2025), while the literature on cybersecurity leadership education highlights competence beyond technical expertise (Anderson et al., 2024).

A PPAIP must be considered an emergent cyber-governance object, rather than just a privacy preference. There may be many questions for a cyber leader to raise about whether an organization's AI profile can be safely transferred, whether there are any exit clauses for the vendor, whether there are any restrictions imposed on retained profiles once employment is

terminated, whether the imported profiles can be trusted, whether identity and provenance are guaranteed, and whether the provider uses any interoperability standards.

The new world of governance is also the place where standards, supervision, revision, and accountability come into play as concerns of leadership. Procurement, vendor evaluation, data governance policies, contracts, and incident response planning all might generate a need for interoperable and accountable processes even before the law reaches maturity. The challenge of anticipatory leadership is not prediction, but simply recognizing the dependency before the choice is no longer possible.

CONCLUSION

Persistent memory of AI is evolving personalization into an asset for a durable relationship. The current literature on portable memory, sovereignty, portability of data, and personal data stores provides essential building blocks; however, the current governance framework is still fragmented, with governance existing across legal, technical, platform and institution levels.

In this paper, we introduce the concept of the Persistent Personal AI Profile as a new governance object and Immutable Portability as the principle of its governance. The core proposition is stronger than mere export: an individual must have an immutable and inviolable right and ability to download, retain and export the PPAIP in a functional manner, regardless of the state of platform relationship. Exporting the data must be coupled with protection against beneficial use of the PPAIP by the previous provider without a new legal ground.

The difference matters. It is possible to comply with an access request by providing a downloadable archive of data that still leaves the individual trapped due to inability to restore the context outside the platform. Similarly, transferring the copy of the data set does not provide control if the previous platform is allowed to continuously mine the individualized profile.

Portability, then, implies not only file formats, but standards, oversight for compliance, a revision process sufficient to accommodate changing standards, and accountability measures robust enough to offset commercial pressures towards lock in and unilateral action. Portability also implies lifecycle management, because a PPAIP could last well beyond periods of dormancy, incapacitation, death, succession, archival management, destruction, and even economic transfer.

This set of unanswered questions does not indicate that the concept itself is premature. It indicates that governance is early. Government actors, standards organizations, technology

suppliers, cybersecurity experts, legal scholars, economists, privacy theorists, and estate law specialists all have a chance to determine the framework before decades of personalized AI contexts are locked inside proprietary systems.

The question to be governed is no longer just whether AI systems should keep memories of people. It is whether people can keep control of the memories about them in persistent digital profiles.

ACKNOWLEDGMENT

The following generative artificial intelligence applications have been used to aid in research and editing: literature search, source search and structuring, research synthesis, manuscript structuring, and language improvement. Concepts, questions, analytical links, arguments, interpretations, conclusions, and scholarly positions have been formulated by the authors. AI-generated content has been reviewed, criticized, modified, and included if it captured the authors' intended message.

REFERENCES

- Anderson, A., Ahmad, A., & Chang, S. (2024). Case-based learning for cybersecurity leaders: A systematic review and research agenda. *Information & Management*, 61, 104015. <https://doi.org/10.1016/j.im.2024.104015>
- De Hert, P., Papakonstantinou, V., Malgieri, G., Beslay, L., & Sanchez, I. (2018). The right to data portability in the GDPR: Towards user-centric interoperability of digital services. *Computer Law & Security Review*, 34, 193–203. <https://doi.org/10.1016/j.clsr.2017.10.003>
- European Parliament & Council of the European Union. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation), Article 20.
- European Parliament & Council of the European Union. (2023). Regulation (EU) 2023/2854 on harmonised rules on fair access to and use of data (Data Act).
- European Parliament & Council of the European Union. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).
- Fallatah, K. U., Barhamgi, M., & Perera, C. (2023). Personal Data Stores (PDS): A review. *Sensors*, 23, 1477. <https://doi.org/10.3390/s23031477>
- Federal Trade Commission. (2020). Data to go: The FTC's workshop on data portability—Summary. Federal Trade Commission.
- Gines, D. (2026, February 17). Portable AI Memory (PAM) specification v1.0. <https://portable-ai-memory.org/spec/v1.0/>
- Google. (n.d.). Download your Gemini Apps data. Gemini Apps Help. <https://support.google.com/gemini/answer/16920332?hl=en>

- Guston, D. H. (2014). Understanding 'anticipatory governance'. *Social Studies of Science*, 44, 218–242. <https://doi.org/10.1177/0306312713508669>
- Hothi, S. (2026). Personal AI sovereignty: From platform data extraction to user-controlled artificial intelligence. SSRN. <https://doi.org/10.2139/ssrn.7335879>
- Microsoft. (n.d.). Manage your Copilot activity history in the privacy dashboard. Microsoft Support. <https://support.microsoft.com/en-US/Privacy/manage-your-copilot-activity-history-in-the-privacy-dashboard>
- OECD. (2024). Framework for anticipatory governance of emerging technologies (OECD Science, Technology and Industry Policy Papers, No. 165). OECD Publishing. <https://doi.org/10.1787/0248ead5-en>
- OpenAI. (n.d.). Exporting your ChatGPT history and data. OpenAI Help Center. <https://help.openai.com/en/articles/7260999-how-do-i-export-my-chatgpt-history-and-data>
- OpenAI. (n.d.). How to delete your account. OpenAI Help Center. <https://help.openai.com/en/articles/6378407-how-do-i-delete-my-account>
- Pentland, S., South, T., Greenwood, D., Pei, J., He, Z., & Moskowitz, B. (2026, March 16). The future of personal AI: Portable and persistent personal memory through a unified human context protocol. Stanford Digital Economy Lab. <https://digitaleconomy.stanford.edu/publication/the-future-of-personal-ai-portable-and-persistent-personal-memory-through-a-unified-human-context-protocol/>
- Perplexity. (2026, July 28). Account deletion. Perplexity Help Center. <https://www.perplexity.ai/help-center/en/articles/10354879-account-deletion>
- Ramezan, C. A. (2025). Understanding the chief information security officer: Qualifications and responsibilities for cybersecurity leadership. *Computers & Security*, 152, 104363. <https://doi.org/10.1016/j.cose.2025.104363>
- Sahin, Z., & Vance, A. (2025). What do we need to know about the Chief Information Security Officer? A literature review and research agenda. *Computers & Security*, 148, 104063. <https://doi.org/10.1016/j.cose.2024.104063>
- Uniform Law Commission. (2015). Revised Uniform Fiduciary Access to Digital Assets Act.
- U.S. Government Accountability Office. (2019, January). Internet privacy: Additional federal authority could enhance consumer protection and provide flexibility (GAO-19-52). <https://www.gao.gov/products/gao-19-52>