

# Self control in a digital age

Paul Trevithick, The Mee Foundation

March 27, 2023. Revised April 23, 2023

## Abstract

We propose a set of individual rights designed to give people control over their online personal information. We show how these rights be implemented by through a combination of user agent technology, licensing contracts, and enforcement by a trusted intermediary organization.

## 1 Introduction

John Locke is commonly regarded as the originator of “self-ownership”—the idea that humans have a property right in their person. In 1689 he wrote, “Every man has a property in his own person: this nobody has any right to but himself.”[4]. The self-ownership that Locke believed was self-evident in the seventeenth century does not obtain in the digital realm.

Hundreds of year later and despite strengthened privacy regulation, we still have little control over our digital selves. Almost all of our human information (e.g., our preferences, interests, affiliations, friends, medical records, location data) is collected, and held by external organizations that effectively have control over it. Often it is held, bought, sold, and leveraged for corporate economic advantage[9]. The resulting loss of privacy and lack of control over our personal data is well-known, despite our belief that having control over our digital selves is vitally important to the future of civil society and democracy.

Our primary goal in this paper it to define a set of personal rights which establish an individual’s control over their personal data<sup>1</sup>. Our secondary goal is to increase the relative power of individuals compared to that of the digital service providers who collect and process this individual’s personal data.

We will propose a set of very specific rights that are tightly coupled with technical mechanisms to implement them (e.g. APIs, user agents, etc.), that together overcome the limi-

---

<sup>1</sup>By personal data we mean any information which are related to an identified or identifiable natural person.

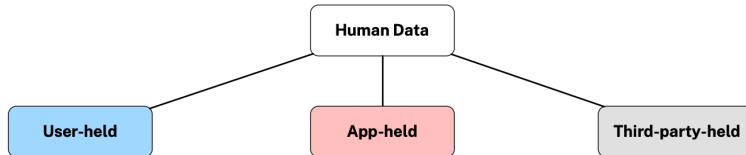


Figure 1: Where personal information is stored

tations of traditional privacy rights alone—limitations that Solove has recently described[7] as follows:

...[E]ffective privacy protection involves not just facilitating individual control, but also bringing the collection, processing, and transfer of personal data under control. Privacy rights are not designed to achieve the latter goal, and they fail at the former goal.

Before we proceed, we define three distinct kinds of personal data based on their locations. Figure 1 shows and names three distinct storage locations for personal information. If it is stored on an individual’s own devices (and not in the cloud) we call it *user-held*<sup>2</sup>. If it is stored by a digital service provider with which the individual interacts we refer to it as *app-held*. We refer to the provider’s mobile app or website as simply an *app*. Lastly, if it is held by third-parties (e.g. data brokers, etc.) with which the user doesn’t directly interact and about whom they are likely not even aware.

## 1.1 Rights for User-held Data

Although it seems natural that individuals should own data about themselves, this is far from settled in the American and European legal literature.<sup>3</sup> Further, creating a property

<sup>2</sup>Our definition narrows Jurcys et al.’s original definition[2]

<sup>3</sup>“Until recently the prevailing approach in the European and American legal literature has been to deny the idea of exclusive data ownership. The widely accepted view has been that such a justification for conferring data ownership rights did not and cannot exist, is not yet proven, is “unlikely to provide the level of control wished for”, and that “the courts are yet to discover it.” The leading legal experts suggested that there was no legal principle or theory that would per se justify the allocation of exclusive property rights over data. Therefore, any recognition of a new property right, such as an ownership right in (personal or non-personal) data, would require an additional and sound justification. One of the main reasons for such a position has been the fact that the notion of (personal) “data” was not specifically defined or was discussed in rather abstract terms.”[2] Other examples include, RadicalxChange.org’s (<https://radicalxchange.org>) Data Freedom Act (<https://www.radicalxchange.org/media/papers/data-freedom-act.pdf>), which is “...informed by a model of social, overlapping claims to data. This view of data, which challenges more familiar notions of individual data ownership, is echoed by top researchers in the fields of data privacy, security, and network economics.” See also the Technium Data Manifesto <https://kk.org/thetechnium/data-manifesto/> whose first tenet reads, “Data cannot be owned. By anybody.” Data cannot be owned, but must be governed.”[5]

right in personal data may be objectionable to those who consider information privacy to be a fundamental civil right<sup>4</sup>.

Despite the challenges of the data-as-property approach for data “at a distance” it applies naturally to when the individual holds data on their own device. The device’s hardware and software architecture implement data processing capabilities which we describe here in the language of a set of “rights”:

- **Collect, Create.** The right to collect or create information about themselves.
- **Access, Update, Delete.** The right to access, update and/or delete their data.
- **Process.** The right to process their data. This includes leveraging it with *local* applications, algorithms, and “personal AI” that process it by direct access to the datastore and without creating remote copies.
- **Share.** The right to share data with other entities.

## 1.2 Rights for App-held Data

App-held personal information is data that a provider has collected through (i) interactions between the user of the data custodian’s app, or (ii) through observations made by the app or associated sensors, or (iii) through data generated by the app as direct byproduct of these interactions, but excluding (iv) data inferred about the individual based on these interactions. App-held data in (i) above includes both information that the user may have shared manually (e.g. by filling in a form), as well as via a user agent.

We propose the following user rights for app-held data:

- **Consent.** The right to require opt-in consent to all collection, transfer, disclosure, retention and use, as well as the right to knowledge of the data custodian’s purpose for each of these.
- **Access, Update, Delete.** The right, to access update, and delete app-held data held by the data custodian.

Traditional privacy law does not recognize the rights above<sup>5</sup> so instead we rely on an approach put forward by Samuelson[6]<sup>6</sup> that relies on intellectual property licensing.

---

<sup>4</sup>As Samuelson has written, “A person may have a civil liberty interest in voting or speaking freely on issues of public importance in a public forum. These civil rights may be legally enforceable, but they are not commodifiable interests akin to property rights. If information privacy is a civil right, it may make no more sense to propertize it than to propertize voting rights to protect the franchise.” [6]

<sup>5</sup>They have similarities to the ‘In-situ’ Data Rights proposed by Van Alstyne et al.[1].

<sup>6</sup>Also advocated by Zittrain[8, p225]

### 1.3 Human Information License

The specific legal mechanism we propose is the Human Information License (HIL)<sup>7</sup>. The HIL is a contract between two parties. The first is the digital service provider which in this contract is referred to as a *data custodian*. The second an organization that represents the community of agent users. This organization is a *Mediator of Individual Data* (MID), a term coined by Lanier et al.[3], that enforces the terms of the HIL on behalf of the user community.

The HIL imposes obligations on the provider to respect the above rights, but it also dictates the technical means by which this must be done. It requires the provider to implement *data rights* application programming interfaces (APIs) that the agent uses to remotely control this app-held data.

The HIL’s provisions are intentionally generic. They are designed to meet the needs of the entire community of agent users. We expect that other contracts containing more specific provisions will be required to meet the needs of more specialized communities. Groups of user communities can amend the HIL to meet the specifics they require, provided that they do not weaken the HIL’s existing provisions and protections. These specialized communities would organize, govern and operate independent MIDs that enforce their more specialized HIL-based contracts. These specialized MIDs would enter into agreements with one or more providers which would be held to both the generic terms of the HIL as well as the additional, specialized terms.

## References

- [1] Marshall W Van Alstyne, Georgios Petropoulos, Geoffrey Parker, and Bertin Martens. ‘in situ’ data rights. *Communications of the ACM*, 64:34–35, 2021. URL: <https://cacm.acm.org/magazines/2021/12/256948-in-situ-data-rights/fulltext>.
- [2] Paulius Jurcys, Christopher Donewald, Mark Fenwick, Markus Lampinen, Vytautas Nekrošius, and Andrius Smaliukas. Ownership of user-held data: Why property law is the right approach. *JOLT*, 2021. URL: <https://jolt.law.harvard.edu/digest/ownership-of-user-held-data-why-property-law-is-the-right-approach>.
- [3] Jaron Lanier and E Glen Weyl. A blueprint for a better digital society. *Harvard Business Review*, 26, 2018. URL: [http://eliassi.org/lanier\\_and\\_weyl\\_hbr2018.pdf](http://eliassi.org/lanier_and_weyl_hbr2018.pdf).
- [4] John Locke. *Second treatise of government: An essay concerning the true original, extent and end of civil government*. John Wiley and Sons, 2014.

---

<sup>7</sup>[docs.google.com/document/d/13aGk5adoncMxxfl5637NfqP6fl6q\\_op\\_1CF50UrJNjg](https://docs.google.com/document/d/13aGk5adoncMxxfl5637NfqP6fl6q_op_1CF50UrJNjg)

- [5] Matt Prewitt. A view of the future of our data: Welcome to the era of data coalitions. *Noema Magazine*, 2 2021. URL: <https://www.noemamag.com/a-view-of-the-future-of-our-data/>.
- [6] Pamela Samuelson. Privacy as intellectual property. *Stan. L. Rev.*, 52:1125, 1999.
- [7] Daniel J. Solove. The limitations of privacy rights. *SSRN Electronic Journal*, 2 2022. URL: <https://papers.ssrn.com/abstract=4024790>, doi:10.2139/SSRN.4024790.
- [8] Jonathan Zittrain. *The future of the internet—and how to stop it*. Yale University Press, 2008.
- [9] Shoshana Zuboff. *The Age of Surveillance Capitalism*. Profile Books, 2019.

DRAFT