Self control in a digital age

Paul Trevithick, The Mee Foundation

March 27, 2023. Revised April 14, 2023

Abstract

We propose a set of individual rights to give individuals control over their online personal information. We show how these rights be implemented by through a combination of user agents, contracts, and enforcement by a trusted intermediary.

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."[3]. This idea was taken up by the American revolutionaries, and was instrumental in justifying their passion to be self-sovereign citizens rather than subjects of a king.

The self-ownership that Locke believed was self-evident in the seventeenth century does not obtain in the digital realm. Despite improvements in privacy laws, we still have little control over our digital selves. Almost all of our human information (e.g., 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 the corporation's economic advantage, not ours[8]. The resulting loss of privacy and lack of control over our personal data is well-known. Owning our digital selves is vitally important to civil society and the survival of democracy in a digital age.

This paper's goal is to give people more control over their *digital* selves, i.e. their personal data[1]. It proposes a set of personal rights which establish people's control over their personal information, just as private property law gives individuals power over their belongings. A secondary goal is to increase the power of individuals relative to that of the digital service providers who collect and process their personal data.

[1]By personal data we mean any information which are related to an identified or identifiable natural person.

By proposing a set of rights that are tightly coupled with technical implementation and enforcement (e.g., APIs and protocols), we hope to address the limitations of traditional privacy rights, limitations that Solove[6] has recently described as follows:

> The main goal of providing privacy rights aims to provide individuals with control over their personal data. However, effective 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.

Despite the fact it seems natural that individuals should own data about themselves, this is far from settled in the American and European legal literature.[2]. Creating a property right in personal data may also be objectionable to those who consider infomration privacy to be a fundamental civil right[3]

Samuelson[5] has proposed[4] an alternative to the data-as-property approach. In it, intellectual property licensing provides the individual with a protectable right, enforced through contract, to control their information.

Figure 1 shows the three locations where personal information is stored. A data-as-property approach is applied to *user-held* data and a contractual, licensing approach to *app-held* data. Unfortunately, a contractual approach is not applicable to *third-party-held* data collected and held by third-parties with which the user doesn't directly interact and about whom they are likely not even aware.

[2] "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."[4]

[3] 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."[5]

[4] Also advocated by Zittrain[7, p225]

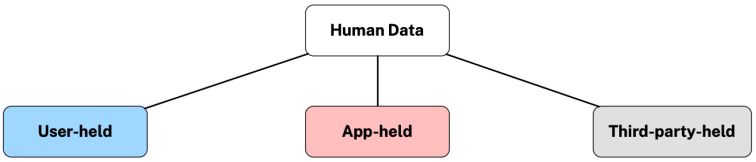

Figure 1: Where personal information is stored

1.1 Rights for User-held Data

We define user-held personal information is data about an individual that the individual can aggregate and store in a personal datastore whether this datastore is located on a personally owned edge device, such as a phone or laptop, or in a personal cloud.[5]. Jurcys et al.[2] argues that the ownership and property rights apply to personal information stored in a personal cloud.

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

- **Collect, Create**. The rights 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."
- **Share**. The right to share data with others without a license. Note that exercising this right undermines ownership, often entirely.
- **License**. The right to transfer a copy of the data to a Data Custodian's app/site, whereupon that copy, becomes *app-held*

1.2 Rights for App-held Data

App-held data is personal information about an individual that is held (stored) by a digital service provider's mobile app, desktop app, or website with which the individual interacts directly. We call these first-party providers, *data custodians*.

We define app-held personal information as data that the data custodian has collected through (i) interactions between the individual 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.

[5]Our definition extends Jurcys et al.'s original definition[2] to edge devices

In all cases these rights must be enforced by a direct digital communication channel between the data custodian and the user's user agent.

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

- **Opt-in**. 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 behind each of these.
- **Access, Update, Delete**. The right, to access update, and delete app-held data held by the data custodian.

'In-situ' Data Rights proposed by Van Alstyne et al.[1] are closely related to the app-held data rights we propose above.

2 Enforcement in code and law

The rights we've outlined can be implemented and enforced using a combination of legal and technical means.

2.1 User-held data rights

Code. The proposed user-held rights, other than the license right, are partially enforced by the hardware and software technology of a personal datastore. In the license right, the data transfer itself is a straightforward technical matter, but it must be performed under the terms of what we call a *Human Information License*(HIL), with the recipient acting as a *data custodian* for the individual to retain ownership over it once it becomes app-held.

Law. If we limit user-held data to data stored on a persons's device, the user-held rights above, other than the License right, can be enforced by code running on the same device and there is no need for additional law. The License right, on the other hand, is enforced by the HIL.

2.2 App-held data rights

Code. A user agent can invoke APIs implemented by the data custodian's app/site to enforce app-held rights.

Law. Privacy laws do not recognize the app-held rights we've described[6] and instead we rely on intellectual property contract law.

[6]The situation is in reality even more stark. Putting aside the rights we propose here, individual data ownership rights are not recognized in any jurisdiction.

2.3 HIL enforcement

A HIL license can be executed between a trusted intermediary (perhaps a nonprofit) operating on behalf of the individual user on the one hand, and the first-party (*data custodian*) on the other. This intermediary organization is responsible for enforcement of the terms of the HIL on the individual's behalf.

3 Conclusion

We have described a system of rights that give individuals control over their personal information online that can be implemented and enforced through a combination of user agent technology, licensing contracts, and a trusted intermediary.

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] John Locke. *Second treatise of government: An essay concerning the true original, extent and end of civil government*. John Wiley and Sons, 2014.

[4] 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/`.

[5] Pamela Samuelson. Privacy as intellectual property. *Stan. L. Rev.*, 52:1125, 1999.

[6] 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`.

[7] Jonathan Zittrain. *The future of the internet–and how to stop it*. Yale University Press, 2008.

[8] Shoshana Zuboff. *The Age of Surveillance Capitalism*. Profile Books, 2019.