You Are the Product—But Do You Own the Data?

New York Law Journal Online
May 7, 2025

When Jessie downloaded a fitness app to track her daily runs, little did she realize that she was creating valuable data points that would be aggregated, analyzed, and sold to advertisers.

Though she inputed her heart rate, routes, and personal health information, does Jessie actually own this data? Can she demand its deletion or prevent its sale? These questions highlight the growing tension between personal data and property rights in the digital age.

The Data Ownership Dilemma

In today's digital economy, personal data has become an incredibly valuable commodity — there are companies that profit from this information — and the question remains: do you actually own your own data?

This distinction matters. When you post on social media, track your fitness on an app, or simply browse websites, you generate data that companies collect, analyze, and monetize. The average American's personal data is estimated to be worth as high as $500 - $7,000 annually to data brokers and technology companies. Without established ownership rights, individuals have limited control over how this information is used or who profits from it.

What Does “Data Ownership” Actually Mean?

According to the United States Office of Research Integrity, at least as it pertains to research, “[d]ata ownership refers to both the possession of and responsibility for information. Ownership implies power as well as control. The control of information includes not just the ability to access, create, modify, package, derive benefit from, sell or remove data, but also the right to assign these access privileges to others.”

However, the question persists as to whether the personal data that you submit for public consumption is something over which you can claim legal ownership - and, further, whether you can exclude others (such as popular social media platforms) from profiting from, or using such data without your consent?

The Legal Framework: Can Data Be Property?

Americans are afforded certain inalienable rights (*i.e.,* freedom of speech, rights to due process, and equal protection under the law), and while privacy is implied in our constitutional framework, our legal system has struggled to clearly define data ownership rights in the digital age.

This gap is not surprising. Concerns about data protection emerged alongside the rise of internet technologies, which were not contemplated when our fundamental human rights frameworks were established. This has created a legal gray area where many argue that the right to privacy in the digital age should be treated as a specific legal right to be defined and regulated, rather than assumed to be covered by existing fundamental rights principles.

A salient case which deals with common law conversion and whether it applies to intangibles is *Kremen v. Cohen*, 337 F.3d 1024, 1029-30 (9th Cir. 2003) (California conversion law). To make out a claim for conversion, one must show a property interest in the thing converted. *Id.*

Property is a broad concept that includes every intangible benefit and prerogative susceptible of possession or disposition….We apply a three-part test to determine whether a property right exists: "First, there must be an interest capable of precise definition; second, it must be capable of exclusive possession or control; and third, the putative owner must have established a legitimate claim to exclusivity." Id.

Application of this test suggests that a set of personal data can, indeed, be a form of personal property:

(a) *it can be defined precisely*—the data points for certain types of information (name, address, credit card number, heart rate, etc.), or more precisely, the association of particular data points (average heart rate) with particular identifying information (name), and their inclusion in a set of data about the person;

(b) *it is capable of exclusive control*; and

(c) *it is based on a legitimate claim to exclusivity*—for instance, where the data pertains to a particular person and the person creates a data set about themselves by inputting their data into an app where it was stored in a database and associated with their identity then the data set was created through the efforts of the person over a period of time.

Legislative Approach to Data Rights

Support for treating data as property can be found in the California Consumer Privacy Act of 2018 (the "CCPA"), Cal. Civil Code 1798.100, *et seq.* The CCPA (which went into effect in January 2020), grants individuals the right to require businesses that collect their personal data the right to control that data—including the right to require deletion of that data, and/or to bar sale of the data to third parties. *See Id.* at 1798.105, 1798.120.

Notably, the CCPA contains a comprehensive definition of personal information: "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household," and then goes on to list twelve (12) categories of such personal information. Cal. Civ. Code §1798.140(v).

Case Law: Evolution of Data as Property

While *Kremen* suggests a path forward for treating data as property, subsequent cases show the limitations of applying that logic to all digital assets. In the 2024 case, *Best Carpet Values, Inc. v. Google, LLC*, 90 F.4th 962 (9th Cir. 2024), the Ninth Circuit decided against extending *Kremen "*to protect as chattel the copies of websites displayed on a user's screen," because the plaintiffs did not allege a cognizable property interest in the website copies nor did they allege a possessory interest sufficient to give rise to a trespass to chattels claim. *Id.* at 968.

Best Carpet is to be distinguished from *Kremen* because the above mentioned three prong test was not satisfied in *Best Carpet*. Moreover, in *Kremen*, the Ninth Circuit determined that

California's conversion law applied to an internet domain name, rather than to the website itself or other intangible assets associated with the website.

A few cases have held that there is no property interest in personal data. *See Low v. LinkedIn Corp.*, 900 F.Supp.2d 1010 (N.D. Cal. 2012) and *In re iPhone Application Litig.*, 844 F.Supp.2d 1040 (N.D. Cal 2012), but these cases have little analysis and seem to rely on older cases. Making the negative impact on this notion even more tenuous is that the two older cases cited in *iPhone* do not even discuss *Kremen*, and in fact deal with a different issue. *See Thompson v. Home Depot, Inc.*, 2007 U.S. Dist. LEXIS 68918 (S.D. Cal. 2007) and *In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705 (N.D. Cal. 2011).

Those two cases dealt with a claim under California's unfair competition law, Bus. & Prof. Code 17200, and the requirement that the plaintiff "suffered injury in fact and...lost money or property as a result of the unfair competition." Both held that merely providing personal information, without more, does not establish a loss of property. Thus, while courts have been reluctant to recognize a loss of property under unfair competition law claims in the absence of economic harm, this should not foreclose the broader inquiry into whether personal data itself is property—especially when it generates commercial value for others.

These cases are distinguishable—merely providing one's personal information does not cause a loss of property, since the person still has the information; however, that does not mean there is no property in the information, and in its commercial exploitation.

The *iPhone* case did cite and purport to apply *Kremen*, but it is not that persuasive. First it held that personal data is not capable of precise definition. But it is not understood why a set of data about a particular person could not be precisely defined. A data set that includes identifying information (*e.g.,* name and social security number) and private information (*e.g.,* weight, heart rate over time, blood sugar readings) are a precisely defined list for that person.

The *iPhone* case also held that "it is difficult to see how this broad category of [personal] information is capable of exclusive possession or control." But, again, given that consumers have the right to demand their information be deleted, or not sold to third parties, this is unconvincing.

Competing Interests: Balance Privacy with Innovation

Some argue that the underlying tensions of control and access in the data privacy discussion may need to be balanced against other societal interests, like national security, public safety, and technological innovation.
David Kris (2016). *Digital Divergence* [White paper]. National Constitution Center. In this view, data privacy is important, but it must be weighed against the need for security, law enforcement, or the benefits of technological development. This is why some governments and institutions may not fully recognize data privacy as a non-negotiable right.

The Path Forward: What's Next for Data Ownership

The current legal landscape concerning individuals' rights to their personal data shared online remains uncertain. As we progress further into the digital age, many people are starting to demand greater transparency regarding the use, storage, and sharing of their personal data.

This growing movement may lead to more legal actions aimed at compelling courts to exploring this issue in depth and providing clearer guidance.

Moreover, emerging decentralized frameworks like Solid (Social Linked Data) illustrate how individuals could host personal data in self-sovereign “pods,” granting apps limited, revocable access without relinquishing ownership.

Additionally, as elected officials receive increasing feedback from constituents dissatisfied with how their personal data is managed, it is likely that more states will feel compelled to enact their own versions of strong data privacy legislation similar to the CCPA.

Milton Springut *is a partner at Herrick, Feinstein in its litigation department and intellectual property and technology group.* **Jermaine A. Brookshire, Jr.** *is an associate at the firm.*
