BROOKINGS

TechTank

Why data ownership is the wrong approach to protecting privacy

Cameron F. Kerry and John B. Morris Wednesday, June 26, 2019

Editor's Note:

The Center for Technology Innovation will be hosting an event titled "Information-sharing ecosystems: How they operate and what that means for privacy legislation" at the Brookings Institution on June 27 at 1:30 PM. RSVP here to attend the event in person.

"It's *my* data." It's an idea often expressed about information privacy.

Indeed, in congressional hearings last year, Mark Zuckerberg said multiple times that "people own all of their own content" on Facebook. A survey by Insights Network earlier this year found that 79% of consumers said they want compensation when their data is shared. Musician and tech entrepreneur will.i.am took to the website of *The Economist* to argue that payment for data is a way to "redress the balance" between individuals and "data monarchs."

Some policymakers are taking such thinking to heart. Senator John Kennedy (R-LA) introduced a three-page bill, the "Own Your Own Data Act of 2019," which declares that "each individual owns and has an exclusive property right in the data that individual generates on the internet" and requires that social media companies obtain licenses to use this data. Senators Mark Warner (D-VA) and Josh Hawley (R-MO) are filing legislation to require Facebook, Google, and other large collectors of data to disclose the value of personal data they collect, although the bill would not require payments. In California, Governor Gavin Newsome wants to pursue a "data dividend" designed to "share in the wealth that is created from [people's] data."

Treating our data as our property has understandable appeal. It touches what the foundational privacy thinker Alan Westin identified as an essential aspect of privacy, a right "to control, edit, manage, and delete information about [individuals] and decide

when, how, and to what extent information is communicated to others." It expresses the unfairness people feel about an asymmetrical marketplace in which we know little about the data we share but the companies that receive the data can profit by extracting marketable information.

The trouble is, it's not your data; it's not their data either. Treating data like it is property fails to recognize either the value that varieties of personal information serve or the abiding interest that individuals have in their personal information even if they choose to "sell" it. Data is not a commodity. It is information. Any system of information rights—whether patents, copyrights, and other intellectual property, or privacy rights—presents some tension with strong interest in the free flow of information that is reflected by the First Amendment. Our personal information is in demand precisely because it has value to others and to society across a myriad of uses.

Treating personal information as property to be licensed or sold may induce people to trade away their privacy rights for very little value while injecting enormous friction into free flow of information. The better way to strengthen privacy is to ensure that individual privacy interests are respected as personal information flows to desirable uses, not to reduce personal data to a commodity.

To unpack the private and public interests inherent in personal information, consider the simple case of your name. It is a fundamental part of individual identity, and it is the first item on any list of "personally identifiable information" protected by privacy rules. We each have vital interest in our names and the assets and identities we link to them.

But this interest is not exclusive. Our names are also a way that others recognize us, associated by friends and family with who and what we are, and used by society for voting rolls, property registries, financial accounts, and countless other social, economic, and civic contexts. This makes our names essential social and economic currency that is valuable to others.

It is because of this social and economic significance that naming is regulated. We are assigned names at birth, registered on birth certificates. It takes official approval to change these names. In this way, as personal as our identities are to us, they are also instruments of a well-functioning society.

Other personal information that we necessarily share alongside our names also involves intersecting interests. The transactions we conduct through a bank become part of the business records of the bank, as the Supreme Court recognized in *United States v. Miller*. But the bank's interest in these records does not necessarily mean it has absolute control to do what it wants with this information, as the Gramm-Leach-Bliley financial privacy law makes explicit. Courts have relied on *Miller* to conclude that records of your cell phone calls and other business records can be obtained from the parties that hold these records.

In *Carpenter v. United States* last year, however, the Court required a warrant for cell phone location data that service providers retain for their use. Although not overturning *Miller*, the Court also recognized that that the phone users retain expectations of privacy in location data generated from their phones. The same intersecting interests apply to much of the other information we share as we interact with digital services—e-commerce transactions, mobile applications, messaging services and other communications, and pictures or information we share on our social networks among others.

Of course, much of the data we generate is shared more widely than just with recipients like these, but here too the interests in information from the data are not exclusive. The digital economy operates in broad ecosystems of data-sharing for diverse uses. Well-accepted examples are for credit reporting; bank clearing and compliance with know-your-customer rules; fraud monitoring; and security. Many of these functions are recognized explicitly in laws and standards—from the first federal privacy law in 1970, the Fair Credit Reporting Act, to the recent European Union General Data Protection Regulation (GDPR) and California Consumer Privacy Act—while others are invisible. Few sectors exist entirely outside such ecosystems. And as businesses outsource functions and move their data processing onto cloud services and remote sensing of all kinds begins to deploy across environments, an increasing amount of personal data is in the custody of entities unknown to us as consumers.

The most visible and debated of these ecosystems are in advertising and marketing. They are controversial both because the visibility to consumers makes them aware of tracking and data-sharing but also because mechanisms of ad-tech like advertising identifiers and cookies enable tracking across sites and devices, sharing information without our knowledge and sometimes even despite measures we take to avoid such tracking and sharing. In turn, data brokers aggregate and supplement much of this tracking information with other data derived from apps, social media, and public databases. As intrusive as such collection and uses can be, regulation must take into account First Amendment protection, which extends in some measure to advertising, and must recognize for better or worse that advertising supports a wide range of socially useful products and services, including vital news media and other content providers.

In short, a significant amount of data sharing serves important public interests and values. The friction and disruption from any system of payments for data would undermine these interests and values. Yet, these costs would come with little benefit for individual privacy.

Instead, what is needed is to enable the sharing personal information that is useful for our social, economic, and governmental systems while protecting the vital interests that each of us has in our personal information. It is precisely to these ends that we need to move away from our current transactional approach to privacy

The handling of personal information in medical research and other research involving human subjects, detection of disparate impacts and analysis to identify discrimination, and the U.S. census provide examples where sharing of information provides important benefits for society. Most medical research is subject to the Health Insurance Portability and Accountability of 1996 and the Privacy Rule adopted by the Department of Health and Human Services (HHS) that defines numerous categories of personal information and limits how these can be disclosed and shared. Human subject research comes under HHS "Common Rule" that provides for institutional review boards to evaluate the risks to subjects, including their privacy, and how to address these risks.

The Equal Employment Opportunity Commission requires employers to report data that includes gender and race or ethnicity. Without data as to race and other protected categories, discrimination is impossible to detect. Census data is considered important

enough that we compel people to respond, but the law also limits the use of this data to statistical use, a limit so deeply embedded that anyone who handles the data must swear an oath to observe the limit, violation of which is a criminal offense. Consistent with these privacy obligations, the release of census data is vetted mathematically to avoid release of information at levels granular enough to associate data with individuals.

In turn, census data provides a foundation for social science research of every kind, informing government policy at every level, academic research, and business planning and market research. The census documentation of the U.S. population and society is available for free — an information commons created by public policy. It works fairly and consistently with our values because public policy also protects a baseline of protection for individual privacy interests. Baseline privacy requirements for how companies protect individual privacy can do the same in the commercial arena.

Basing privacy protection on property systems, on the other hand, would reduce privacy to a commodity, double down on a transactional model based on consumer choice, and be enormously complicated to implement. The current notice-and-choice model is failing because it is effectively impossible for users to understand either how their data will be used or the accompanying privacy risks, especially in the constant flow of online engagement in today's connected world. The result is that people click past privacy notices through to the information or service they want.

Moreover, many of these consumers already agree to provide personal information in exchange for the perception a benefit. It is hard to imagine people will burrow deeper into privacy disclosures or pause at clicking through to get at communications or transactions simply because they are offered what may amount to a few pennies. It is far from clear that in a market for data, the ordinary user would come out on top—either in relation to economic benefits or privacy harms. On the contrary, by licensing the use of their information in exchange for monetary consideration, they may be *worse* off than under the current notice-and-choice regime.

Indeed, the uncertainties of valuating any one individual's data suggest that individuals will receive little payment. Estimates vary but *The Financial Times* has a calculator that one of us (Kerry) ran for his profile. The default value is $0.007, but as a well-to-do professional who travels a lot, the value of the Kerry data was estimated as $1.78. If pricing is set by service providers, then the resulting system is likely to end up being very similar to the current "take it or leave it" outcomes that are common under notice and choice. If pricing is set by consumers or through negotiation, the complexity of the service-user interactions would be even greater. And this new complexity would likely slow users' access to information and services that they want—and simply turn "click fatigue" into "negotiation fatigue."

If pricing is set by regulators or a legislature, this could require drawing of lines about the use of information based on judgments that some should be favored and others disfavored (e.g., different pricing for medical research versus commercial data brokerage). Yet this approach might risk an adverse review under the Supreme Court's First Amendment holding in *Sorrell v. IMS Health Inc.*, which rejected a Vermont limitation on a few particular uses of information about a pharmacy prescription transaction. Although the *Sorrell* case turned on particular decisions and statements made by the Vermont legislature, any privacy legislation is likely to face challenges under the First Amendment commercial speech doctrine, which encompasses commercial advertising within free speech protection on the basis of a "strong interest in the free flow of commercial information" on the part of both consumers and society. It is far from clear that a property rights approach to privacy would improve the arguments needed to withstand a constitutional challenge on such grounds.

A property-based system also disregards interests besides property that individuals have in personal information. Consumers often benefit from freely providing information for use in a particular context, but they can suffer a range of privacy harms if the information is used in an unrelated context not contemplated when use of the information was licensed. At the same, imbuing property rights in personal information would affect sharing of data in many common contexts. In a simple purchase of a book from an online

retailer, for example, the book title and subject could reveal highly personal information about the purchaser, but the retailer surely would have a right to retain and use its own business records about the transaction (including the title of the book).

Under an information-as-property regime, would both the purchaser and the retailer have property rights to information about the transaction? And in such a property regime, couldn't the retailer simply make as a condition of sale that the purchaser must grant a license to the retailer to use the information for specified uses? And wouldn't that simply lead to another form of the tyranny of fine print in which the purchaser who wants the convenience of an online purchase would be forced to cede rights to the retailer? It is unclear whether the information as property regime would in fact improve the current state of privacy.

Looking beyond this retail scenario, how would information-as-property apply to a simple online conversation between two individuals who exchange personal information with each other—perhaps even information about personal activities that the two individuals did together? Would both individuals have property interests in the personal information about a joint activity? Would that mean that neither individual could tell anyone else about the joint activity without the permission of the other individual? (Facebook allows users to delete or port their own photographs but not other people's photos in which they are tagged).

The European Union's GDPR provides a benchmark for the complexity of introducing property interests into information ecosystems. The regulation required an enormous amount of systems design work to map data flows within organizations, document these for regulators, change user interfaces, and create the back-end systems to enable individual access, correction, and deletion. Microsoft revealed that it put 1,600 engineers on the task implementing the GDPR. Creating a system of micropayments similarly would add major new layers to user interfaces and back-ends systems.

There are apps and proposals that seek to protect privacy through intermediaries. MIT's big data pioneer Alexander Pentland and Thomas Hardjono have proposed that credit unions and labor unions could use their collective role to operate data cooperatives on behalf of their members, negotiating and managing permissions as well as deriving

insights for their users. In a similar vein, CitizenMe is developing a data "exchange" that enables individuals to pool their data for surveys and other uses in exchange for compensation, and also to receive develop analysis of their data. In time, a privacy marketplace may develop platforms like these. In the meantime, the challenges of implementation, adoption, and permissions management across many different contexts and interests in information means these are not a substitute for widely applicable baseline privacy legislation.

Alan Westin's insight about control has a place of honor in the constellation of individual interests that make up what we call privacy. But it should not be taken literally as the entirety, it cannot be exclusive, and it is not enough to protect interests that persist in personal information even after we share it with others.

Privacy legislation should empower individuals through more layered and meaningful transparency and individual rights to know, correct, and delete personal information in databases held by others. But relying entirely on individual control will not do enough to change a system that is failing individuals, and trying to reinforce control with a property interest is likely to fail society as well. Rather than trying to resolve whether personal information belongs to individuals or to the companies that collect it, a baseline federal privacy law should directly protect the abiding interest that individuals have in that information and also enable the social benefits that flow from sharing information.