Insight

The Law & Economics of "Owning Your Data"

WILL RINEHART | APRIL 10, 2018

In the wake of revelations about data misuse at Facebook, some are looking to individual data ownership as a worthwhile policy to promote greater competition among tech companies and higher personal-data security. That individuals should "own their data" seems, on the surface, to be a sensible path. This concept of data ownership, however, papers over a more complex set of legal and economic questions.

The properties of data make ownership a difficult prospect. Knowing this, regulators have instead opted for simple restrictions on data use instead of making data completely an individual's property. Consumer behavior confirms part of this thesis, as many are willing to trade their information for services. Not surprisingly, data ownership, like other data restriction plans, is a costly endeavor. While there is a natural inclination to push for data-ownership policies, implementing these kinds of policies would have a detrimental effect on innovation.

The Simple Economics of Information

The nature of information makes it difficult to apply the concept of individual ownership. Ownership is typically understood as a bundle of rights, including the exclusive use of an asset. The corollary of this is that an owner is granted a right to exclude others in using it. Combined, both give rise to the right to transfer an asset, by selling it for example.

Real property, such as land, or personal property, such as a car, easily confers these rights, including the right to possess, exclude, and transfer. If someone sells a piece of land, then they vacate the land. Selling a car means you hand over the keys and the title.

Data, in contrast, doesn't hold the same kind of connection between ownership and exclusion that exists for tangible goods. Information isn't easily excludeable, so when person A transmits information to person B, both now have that information. It is hard for person B to ensure that person A is not keeping a copy of that original information. Rather, for this kind of transfer to happen, for person A to be stopped from reproducing that piece of information, they have to be limited in what they can say.

Intellectual property rights rest on this theory of information production. Because information can be easily shared, costly information will face hurdles in being produced. If, for example, a group expects that their $1 billion investment in a drug will be copied by others, then their incentive to undergo that research and development is minimal unless they can easily recoup their costs on the back end.

In key ways, then, data-privacy laws stand in opposition to property rights. Intellectual property rights are a subset of property rights more generally, whichs incentivizes the production and usefulness of information. On the other hand, many instead want to prevent this creation. Privacy laws try to minimize data use and creation. Thus, privacy laws are generally not referred to as property laws. What consumers mean when they say they want data ownership is that they want the ability to limit the creation of information or limit its use.

Privacy regulations on the books and on the ground

While it is underappreciated, the United States does have a privacy regime focused on restricting and policing the use of data. Instead of the broad privacy regulations that other countries have, privacy laws in the United States are narrowly tailored to specific harms. For example, the Health Insurance Portability and Accountability Act (HIPAA) helps to protect the health information of consumers by making an unauthorized transfer of data subject to a fine. The Fair Credit Reporting Act (FRCA) does the same with financial data. The Children's Online Privacy Protection Act (COPPA) erects a barrier for children and again fines companies if they don't comply.

More important than the laws on the books is the enforcement on the ground by the Federal Trade Commission. Indeed, in recent years the FTC has effectively become the Federal Technology Commission.[1] The Commission has brought over 500 enforcement actions in the name of protecting privacy. Its enforcement has addressed spam, issues in social networking, behavioral advertising, pretexting, spyware, peer-to-peer file sharing, and mobile privacy. It has brought enforcement actions against some of the largest tech companies, including Google, Facebook, Twitter, and Microsoft.

Acceptable practices and uses of data by large data collectors come from a combination of statues, FTC suits, and the companies' own desire to minimize potential liability in the future. As Kenneth Bamberger and Deirdre Mulligan, two of the most widely respected privacy scholars, have detailed in a series of articles and in a book, implementing privacy on the ground is very different than what exists in statutes. What they reveal in their extensive review of actual corporate management practices is that *ex post* regulation by the FTC and the efforts of privacy advocates, professionals, and market forces create a more ambiguous legal environment; they call it productive ambiguity. Compliance with procedural measures gets substituted with more substantive ones, leading companies to seek "the vindication of consumer expectations regarding the treatment of personal information."

Because companies know they have to protect consumers and will face punitive actions if they don't, firms are cajoled into implementing substantive protections. The proof lies in the C-suite. U.S. companies, compared to their counterparts in Europe, are staffed up with Chief Privacy Officers and other privacy professionals. The International Association of Privacy Professionals (IAPP) began in the United States and now counts 30,000 members in its ranks. Yet, only about 25 percent of those members are in the EU, while nearly 60 percent are in the United States.

Individual property rights over personal data would thus force a superordinate right over a complex web of international, national, and, in the case of many states, local restrictions. Already, the laws and regulations create huge complications for legal compliance and cooperation across state lines. Adding another set of rights on top of this would restrict the free flow of information even more and add additional burdens to everyone involved.

Granting individual data property rights would also face fierce opposition in the courts. As UCLA Law

Professor Eugene Volokh explained in a seminal paper on this topic, privacy regulations are inherently government restrictions on free speech because they stop speech about a person. For this reason, comprehensive privacy laws have had a tough time in the United States, as compared to Europe. So too, most of the justifications that would undergird privacy speech restraints could be applied to other speech as well. Accepting any kind of reason for restrictions in the name of privacy, which is notoriously difficult to define, would create a powerful precedent for other kinds of restraints and acts as a deterrent to adoption.

The Privacy Paradox

Data ownership claims also conflict with the so-called privacy paradox. In surveys, individuals claim to want privacy protections, but in practice they willingly give information for trivially small amounts of money. When people are given the ability to trade their information for some kind of service, they opt for the service.

One of the going theories explaining this phenomena is called benefit immediacy, meaning the benefits of sharing the information are immediate while the risks are delayed. Because individuals care so much about the present, the benefits outweigh the risks. This explanation comes directly from the behavioral economic literature, which also lays out a solution. Because consumers truly don't know what is being sacrificed on their end, these scholars contend, what consumers choose in the real world isn't evidence enough that they prefer these technologies. Regulators need to step in.

But, this privacy paradox might not be such a paradox, economist Caleb Fuller argues convincingly. One need not rely on a theory where consumers are persistently fooled or behaving inconsistently with their true preferences to explain privacy preferences. Rather, consumers may have "simply a positive preference for more of an economic good, ceteris paribus," knowing what is being given up. As Fuller found in surveying Internet users, nearly 90 percent of those that voluntarily use Google are aware of its business model based in data collection. Like other surveys, 71 percent of respondents said they would prefer not to be tracked, but of this group, 74 percent are unwilling to pay anything to retain that privacy.

In short, people know what kind of business model that platform companies are engaged in and want the benefits of trading their data. At the same time, they also want to restrict its use. Creating property rights won't solve these competing demands of both innovation and restriction.

The Value of Data and the Cost of Privacy Regulations

This tension really comes into focus when estimates of how much people would be willing to pay are considered. Even under generous assumptions, Google could hope to make somewhere between $14 and $15 million dollars per year if it charged a fee. To put that in perspective, the 2017 total revenue for Google's parent company, Alphabet, was $111 billion. Consumers' willingness to buy the service is substantially lower than the willingness of advertisers to place an ad on digital properties.

How much value do people get in return? While it is difficult to measure an intangible good, one method looks at the time people don't spend on other activities. In 2016, American adults spent 437 billion hours consuming content on ad-supported media. All of that time sums to at least $7.1 trillion in terms of foregone wages, hardly a paltry number. In all, this is a good trade.

Making data an individual's property would be a kind of data restriction, and in general, these policies have been shown to be costly. For example, the Information Technology and Innovation Foundation estimated that

the European Union's Cookie Law, which requires that everyone is notified of the use of cookies, comes at a price of nearly $2.3 billion per year and has adversely affected the online news market. When the EU adopted the e-Privacy Directive in 2002, investment by venture capital in online news, online advertising, and cloud computing dropped by between 58 to 75 percent. Similarly, members of the Fortune 500 will spend a combined $7.8 billion to come into compliance with a new European privacy regulation.

Data restrictions hobble the entire ecosystem, making it all that more difficult for firms to work on innovating. For sensitive data types, however, U.S. authorities have rightly adopted laws knowing there will be a cost included in its passage. The FTC, for example, acknowledged that the Children's Online Privacy Protection Act (COPPA) has implementations costs. Indeed, policy makers shouldn't shrink from what has worked in the past—in both the regulations' substance and form. Regulations have historically been tailored narrowly, and both enforcement and regulations should continue to be narrowly tailored to deal with specific harms.

Conclusion

As writer Seth Godin said, "The art of good decision making is looking forward to and celebrating the tradeoffs, not pretending they don't exist." As policy makers consider any new privacy restriction or control regime, they should be concerned about the relevant tradeoffs that their plan would force. In the end analysis, they need to ask whether or not such an imposition actually benefits consumers in the long run. In the case of turning data into personal property, the benefits simply don't add up.

---

[1] Scholars Berin Szoka and Geoffrey Manne coined this term: http://techfreedom.org/the-federal-trade-commission-has-become-the/