Who Owns Your Data?

Gilad Rosner  
Horizon Digital Economy Research Institute  
University of Nottingham, UK  
Gilad.Rosner@nottingham.ac.uk

Abstract  
Popular and professional discussions of personal data are often framed in terms of ownership – that human data subjects own the data they emit and share. This framing has implications for consent concepts. Ownership, however, is an inappropriate way to conceive of personal data – in most cases the law does not grant proprietary interests in much of the personal information that makes up the digital economy. This paper explores the question, “Who owns your data?” from policy, business, legal and philosophical viewpoints, arguing that a new discourse is required for people to understand how much control they actually have over their personal information in order to build a stronger foundation for consent within ubiquitous computing systems.

Author Keywords  
Consent, Ubiquitous Computing, Data Ownership

ACM Classification Keywords  
K.4.1 [Computers and Society]: Public Policy Issues - Ethics

Consumer uses of the internet often involve the collection of personal data. Starting from the view that such data is valuable and sensitive, a critical question emerges: who owns this data? Who owns the so-called
“digital footprints” and personal information people leave as they traverse the real world and the virtual one? Ownership, as shall be shown, manifests in fluid ways, but a central theme emerges: it is the right to determine the use of what is owned to the exclusion of others [5, 14], i.e., exclusive control.

If ownership is tantamount to control, then determining ownership defines who can collect, process, use, and disseminate personal data. Ownership implies rule-setting for data retention – who can store it, for how long, who can destroy it? Owners have the latitude to select the purposes for which data is used; for example, one’s medical data can be used for one’s own health care, but if one owns it, it could be withheld from use in stem cell research. Ownership also can mean the right to profit from what is owned. Resolving the question of “Who owns your data?” is an exploration of the nature of control over private information about people, and an investigation of the concept of personal data as property.

Since the collection of personal information occurs on a grand scale by entities other than the data’s source, ambiguities around ownership could lead to misappropriation and misuse. As ownership is connected to economic value, ambiguities may lead to an undervaluing of data, and a loss of utility by data subjects [15, 16]. The generally low infrastructural cost of obtaining personal data already causes “data hoarding” about individuals by companies [11, p. 4]. Inappropriately low value estimations of data – both in financial terms and with regard to the rights of individuals – may encourage a lax approach to security by the holders of data. Matwyshyn [11] cites estimates of 162 million personally identifiable American consumer records exposed in data breaches in 2007 alone. Further, data hoarding yields a large “attack surface” for information theft [11, p. 5]. Broadly speaking then, ownership of personal data implies a concern for stewardship, and a lack of clearly defined boundaries of ownership can lead to an abrogation of the responsibility to safeguard it.

Terms and conditions and privacy policies for websites exist in part to inform users of the nature of their relationship with data collectors – an essential element for users to be able to meaningfully consent to collection. However, the language used by these organizations increases the ambiguity around data ownership. Twitter’s Terms of Service [17] state: "This license is you authorizing us to make your Tweets available to the rest of the world and to let others do the same. But what’s yours is yours – you own your content...”

The Privacy Policy for the now-defunct Google Health [4], an online health information aggregation service, stated, "[w]e believe that your health information belongs to you, so we put you in control". A report by the UK Centre for Policy Studies was released titled “It’s Ours: Why we, not government, must own our data” [12]. The problem with this language is that “own” and “belongs to” are misleading when describing a relationship with personal data. Without clarity on this point, citizens may hold unrealistic views of the breadth of their control over, and rights in, the information about them. A 2010 study [9] on the differences between older and younger peoples’ views on privacy "found that while young adults tend to be similar to older adults in attitudes, practices, and policy
preferences regarding information privacy, they are quite more likely than older adults to be wrong in judging whether the legal environment protects them.” [13, p. 18]

What is Ownership?
So, what is ownership, and how does one come to own something? Ownership is “a set of relations constituted by rights and duties among persons. There is nothing in the object owned which marks it off as mine, yours, or ours.” [5, p. 3-4]

Grunebaum [5], breaks ownership down into two essential functions: the rules and mechanisms by which the rights of ownership are assigned to someone, and “what owners may do with what they own” (p. 18). Ownership, therefore, is a relationship between society, a person, and a thing. Broadly speaking, owning something confers the exclusive rights to possess, use, and manage that which is owned, and to derive income from it [5]. Further, “[t]he touchstone of a property right is its universality,” states Michael Bridge [2, p. 12], “it can be asserted against the world at large and not, for example, only against another individual such as a contracting partner.” That is, within a given society, if something is deemed to be owned, it creates an exclusive class of the Owner, and a second class of Non-owner for everyone else in the world [5]. A key element of ownership, therefore, is exclusive control – the right to use, profit by, prevent the use of, control access to, sell, and destroy – and the right to remain in control without interference from others [8]. There are limits to these rights, of course, such as the prerogatives of law enforcement and the sale of restricted goods. The state reserves rights for itself as regards property; pure, unencumbered ownership rights do not exist [4].

Ownership of Personal Data
UK and American law do not recognize the existence of a property right in information [2, 7, 15, 16]. They recognize intellectual property rights in intangibles such as music, commercial goodwill [2], and, to a degree, trade secrets, but not information. Hardcastle [6] states: "...it is not yet settled whether English law regards information as capable of a proprietary characterization. The more accepted view is that information is not property." (p. 12)

In "Privacy as Intellectual Property?", Pamela Samuelson [16] writes:"...however intuitively powerful the notion of property rights in one's data may be, it is clear that in the United States the existence of some legally protectable interests in personal data in certain circumstances is not equivalent to a legal rule that a person has a property interest in one's personal data.” (p. 1132)

Facts do not receive intellectual property protection. A central reason is that facts, such as personally identifiable information, are neither "creative" nor "original," which are requirements for copyright protection [7]. So, with regard to personal data – certainly at least the transactional, fact-based kind – it appears that no one owns it. Absent a property right, both people and the collectors of information about them still enjoy various rights and protections, can sue in court for damages, and may be subject to criminal penalties for misuse. But, the defining elements of ownership – the ability to control, destroy and profit from something while excluding the rest of the world
from doing the same – are not available for the data people shed or intentionally deposit as they work, live, and play in the information spaces they inhabit. Contrast this with the creative products of someone’s mind, such as a novel – copyright ensures that no one can distribute or profit by it without explicit permission from its creator. There is no such protection for the data generated by someone’s online activities – shopping, websurfing, searching for information on Google – even though she or he is the data’s source.

The lack of a property right in personal data has a far-reaching impact. Without ownership, the ability to control data derives from various laws, such as the EU Data Protection Act (DPA) and its various national transpositions, privacy laws, personality rights and the ability to enter into contracts with others. As one travels the internet or makes purchases with debit cards, the disposition of the resultant data is determined in great part by the relationship between the data source and the data collector. The use of purchasing information is governed by the card issuer’s agreement; information collected by a website is governed by its privacy policy. While data protection laws like the DPA spell out the responsibilities of data collectors, the relationship between the collector and the source is multifarious. Some scholars believe that an asymmetry exists between individuals and the companies who seek to obtain their data [15]; in other words, people may be at a disadvantage when contracting with businesses with respect to their bargaining power and ability to understand the potential uses of their personal information. The debate on whether granting a property right in personal data would improve privacy is often cast in economic terms [10, 15, 16]. From this emerges the view that the absence of property rights causes personal data to be valued far lower than is appropriate [15, 16]. People do not need to be paid for their data since they do not own it. Moreover, examples like Facebook and Twitter show how willing people are to give data away for free or in exchange for access to a website or service. If a company relies on data collection as its core business or uses the data for financially beneficial activities such as sales, marketing and product improvement, then it is getting this valuable resource without incurring significant cost. It’s as if a mining company did not need to pay for the land from which they extracted minerals. Or, put another way:

“...much like unregulated, polluting factories, businesses collecting large amounts of personal data are able to internalize the gains from using and selling personal data while externalizing most of the negative impact that results from their practices.” [15, p. 277]

It is very difficult to find estimates of the size of market for personal information, in part because it is difficult to frame the search parameters. One small indication of the size is MasterCard’s data warehouse, which in 2008 was 100 terabytes, and was expected to grow to 1.8 petabytes; that’s but one company, and its business relationships with banks and vendors allow the automatic sharing of large swaths of that information [18]. Since the data MasterCard collects are facts – purchases and the like – the contents of their massive warehouse are not ownable, but clearly the data has value. Database rights and copyright protect MasterCard’s investments even though they do not protect the underlying information. There is great value in the aggregation of personal data; as Samuelson [16] notes:
"There is at the moment a 'lively market' in personal data, but it is a market in which individuals play at most a very small role." (p. 1132) Attempts to shift this value inequity are appearing under headings such as 'vendor relationship management' and 'personal data lockers,' though these are at the moment more experiment than sustainable business.

If Not Ownership, Then What?

Discussions of the economic asymmetries of personal data tend to be rarified academic debate rather than large social discussion. However, there is a great deal of evidence for citizen concern with control of information about them [9]. Perhaps, then, ownership is not the appropriate framework from which to address people's anxieties and the broader rights of data protection and privacy. Control regimes and rights are better perspectives from which to consider the state of personal data. Instead of "Who owns your data?" the questions could be "Who controls your data?" and "What are your data rights?" In that case, starting again from the view that the disposition of personal data implicates the social goal of privacy, answering the questions requires a review of the adequacy of data protection laws in meeting that goal. This is a broad task, and one that has been attempted by many [1]. For instance, it has been argued that data protection laws are not truly privacy laws [15]; that they are instead merely a set of fair information principles. After all, Viktor Mayer-Schönberger [13] writes: "It is not 'data' that is in need of protection; it is the individual to whom the data relates." (p. 219)

Corien Prins [15] argues that data subjects under data protection acts do not determine what happens to their data, but data controllers, as long as they act in accordance with its fair information principles, are free to collect, use, control and further process data forever. Prins [15] goes on to say

"In contrast to copyrighted works, the issue of the control of personal data is not so much as to whether personal data are used. Instead, it is about the specifics of the context in which the data are processed as well as the actual uses to which personal data are put." (p. 299, emphasis added)

From these perspectives, one can conclude that collectors of information control personal data to a far greater degree than the individuals who generate it. Moreover, a number of authors have argued that the orientation of data protection – be it through property rights or codes of practice – is an inappropriate way to safeguard privacy [1, 15]. As Phil Agre [1] states: "privacy is not simply a matter of control over data; it also pertains to the regimentation of diverse aspects of everyday life through the sociotechnical mechanisms by which data are produced." (p.18)

Ownership language is therefore harmful to the necessary precursors to consent. Meaningful consent relies on people being informed about the nature and breadth of data known about them, the risks involved in the holding and using that data, and the rights accorded them regarding its control.

The EU's draft General Data Protection Regulation [3], a major updating of the 1995 Data Protection Act, partly captures this issue in the following requirement:
“it should be clarified that consent does not provide a valid legal ground where the individual has no genuine and free choice and is subsequently not able to refuse or withdraw consent without detriment.” (at (33))

Free choice depends on an accounting of risk and available control. The growth of cloud computing, putting more and more data storage and processing in distributed systems owned by a plurality of largely private companies, implies an even greater need to frame informational control in more appropriate terms of rights, contracts and market norms. Efforts to shift the value inequity between data sources and collectors are still in their infancy. They can only benefit from more accurate discourse on the nature of the relationship between people and their data. An emphasis away from the concept of data ownership towards actual control and rights regimes is essential to re-frame discussions of consent.

References
[9] Hoofnagle, C., et al. How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies? SSRN eLibrary, 2010