

ARTICLE

Who Owns My Data?

Peter G. Klein

This month's revelations by Facebook "whistleblower" Frances Haugen have brought renewed scrutiny to Big Tech. Haugen's concerns relate not to the more common antitrust complaints about firms like Apple, Google, Amazon, and Facebook abusing their market position to thwart competition and innovation, but to broader worries that these firms exercise undue influence on public life. Facebook, in particular, is said to control so much of the "public square" that its policies toward content moderation and the promotion of particular kinds of content increase social and political polarization - even affecting the outcome of national elections.

To be sure, such complaints could be (and have been) raised against the traditional media. (Even in the 2020 US Presidential Election the decision of the Associated Press, CNN, and other outlets to suppress the New York Post's reporting on Joe Biden's son Hunter probably had as much influence as anything on Facebook in 2016 or 2020.) There are also concerns about how social media platforms (like Facebook subsidiary Instagram) affect the health of children and teens. Underneath these conversations, however, lies the basic business model used by ad-supported platforms, namely the harvesting of vast amounts of user data to sell targeted ads. These data are also used to increase engagement on the platform (e.g., by controlling how users see particular types of content), all with the ultimate aim of increasing the value of advertising space.

Advertising, even targeted advertising, is hardly new. But the widespread (and indiscriminate) collection of user information raises legal and ethical, as well as economic, concerns. It feels like a violation of privacy. Sure, I clicked "I agree" to the Terms of Service when I signed up or downloaded the app. But did I really consent to have so much of my online activity tracked, compiled, and analyzed?

To answer, we need to think clearly about the nature of digital footprints. Is "my data" something that can be owned and, if so, do I own it? Are tech platforms violating

my privacy? What exactly is “privacy” anyway? Here are some thoughts (about which I wrote previously [here](#)).

First, privacy, like information, is not an economic good. Just as we don’t buy and sell information per se but [information goods](#) (books, movies, communications infrastructure, consultants, training programs, etc.), we likewise don’t produce and consume privacy but what we might call privacy goods: sunglasses, disguises, locks, window shades, land, fences and, in the digital realm, encryption software, cookie blockers, data scramblers, and so on.

Privacy goods and services can be analyzed just like other economic goods. Entrepreneurs offer bundled services that come with varying degrees of privacy protection: encrypted or regular emails, chats, voice, and video calls; browsers that block cookies or don’t; social media sites, search engines, etc. that store information or not; and so on. Most consumers seem unwilling to sacrifice other functionality for increased privacy, as suggested by the small market shares held by DuckDuckGo, Telegram, Tor, and the like suggest. Moreover, while privacy per se is appealing, there are huge efficiency gains from matching buyer and seller characteristics on sharing platforms, digital marketplaces, and dating sites. There are also substantial cost savings from electronic storage and sharing of private information such as medical records and credit histories. And there is little evidence of sellers exploiting such information to engage in price discrimination. ([Aquisti, Taylor, and Wagman, 2016](#) provide a detailed discussion of many of these issues.)

Regulating markets for privacy goods via bans on third-party access to customer data, mandatory data portability, and stiff penalties for data breaches is tricky. Such policies could make digital services more valuable, but it is not obvious why the market cannot figure this out. If consumers are willing to pay for additional privacy, entrepreneurs will be eager to supply it. Of course, bans on third-party access and other forms of sharing would require a fundamental change in the ad-based revenue model that makes free or low-cost access possible, so platforms would have to devise other means of monetizing their services. (Again, many platforms already offer ad-free subscriptions, so it’s unclear why those who prefer ad-based, free usage should be prevented from doing so.)

What about the idea that I own “my” data and that, therefore, I should have full control over how it is used? Some of the utilities-based regulatory models treat platforms as neutral storage places or conduits for information belonging to users. Proposals for data portability suggest that users of technology platforms should be able to move their data from platform to platform, downloading all their personal information from one platform then uploading it to another, then enjoying the same functionality on the new platform as longtime users.

Of course, there are substantial technical obstacles to such proposals. Data would have to be stored in a universal format – not just the text or media users upload to platforms, but also records of all interactions (likes, shares, comments), the search and usage patterns of users, and any other data generated as a result of the user’s actions and interactions with other users, advertisers, and the platform itself. It is unlikely that any universal format could capture this information in a form that could be transferred from one platform to another without a substantial loss of functionality, particularly for platforms that use algorithms to determine how information is presented to users based on past use. (The extreme case is a platform like TikTok which uses usage patterns as a substitute for follows, likes, and shares, portability to construct a “feed.”)

Moreover, as each platform sets its own rules for what information is allowed, the import functionality would have to screen the data for information allowed on the original platform but not the new (and the reverse would be impossible – a user switching from Twitter to Gab, for instance, would have no way to add the content that would have been permitted on Gab but was never created in the first place because it would have violated Twitter rules).

There is a deeper, philosophical issue at stake, however. Portability and neutrality proposals take for granted that users own “their” data. Users create data, either by themselves or with their friends and contacts, and the platform stores and displays the data, just as a safe deposit box holds documents or jewelry and a display case shows off an art collection. I should be able to remove my items from the safe deposit box and take them home or to another bank, and a “neutral” display case operator should not prevent me from showing off my preferred art (perhaps subject to some general rules about obscenity or harmful personal information).

These analogies do not hold for user-generated information on internet platforms, however. “My data” is a record of all my interactions with platforms, with other users on those platforms, with contractual partners of those platforms, and so on. It is co-created by these interactions. I don’t own these records any more than I “own” the fact that someone saw me in the grocery store yesterday buying apples. Of course, if I have a contract with the grocer that says he will keep my purchase records private, and he shares them with someone else, then I can sue him for breach of contract. But this isn’t theft. He hasn’t “stolen” anything; there is nothing for him to steal. If a grocer – or an owner of a tech platform – wants to attract my business by monetizing the records of our interactions and giving me a cut, he should go for it. I still might prefer another store. In any case, I don’t have the legal right to demand this revenue stream.

Likewise, “privacy” refers to what other people know about me – it is knowledge in their heads, not mine. Information isn’t property. If I know something about you,

that knowledge is in my head; it’s not something I took from you. Of course, if I obtained or used that info in violation of a prior agreement, then I’m guilty of breach, and I use that information to threaten or harass you, I may be guilty of other crimes. But the popular idea that tech companies are stealing and profiting from something that’s “ours” isn’t right.

The concept of co-creation is important, because these digital records, like other co-created assets, can be more or less relationship-specific. The late Oliver Williamson devoted his career to exploring the rich variety of contractual relationships devised by market participants to solve complex contracting problems, particularly in the face of asset specificity. Relationship-specific investments can be difficult for trading parties to manage, but they typically create more value. A legal regime in which only general-purpose, easily redeployable technologies were permitted would alleviate the holdup problem, but at the cost of a huge loss in efficiency. Likewise, a world in which all digital records must be fully portable reduces switching costs but results in technologies for creating, storing, and sharing information that is less valuable. Why would platform operators invest in efficiency improvements if they cannot capture some of that value by means of proprietary formats, interfaces, sharing rules, and other arrangements?

In short, we should not be quick to assume “market failure” in the market for privacy goods (or “true” news, whatever that is). Entrepreneurs operating in a competitive environment – not the static, partial-equilibrium notion of competition from intermediate micro texts but the rich, dynamic, complex, and multimarket kind of competition that characterizes the digital economy – can provide the levels of privacy and truthiness that consumers prefer.

Peter G. Klein

Professor of Entrepreneurship at Baylor University’s Hankamer School of
Business.

Citation: Peter G. Klein, *Who Owns My Data?*, CONCURRENTIALISTE (October 18, 2021).