Fiduciary Data Banking: A Market-Based Alternative to Surveillance Capitalism

S. Goldstein[1,1], P. Machalek[1,1]

Abstract

The rise of surveillance-based business models results in a loss of human agency on a massive scale that makes people feel increasingly despondent about their addiction to technology, and cynical that their digital labor enriches a handful of shareholders. Traditional notions of privacy fail to contemplate the proliferation of ways in which data is being extracted from users by Internet platforms. Regulators struggle to come up with legal frameworks to protect against this. We propose a new fiduciary data banking model that radically and aggressively retains consumer agency based on principles of encryption and local storage. Recent developments in the areas of public key cryptography, the blockchain and smart contracts offer useful approaches. Our solution encompasses (1) minimizing personal data exposure (2) managing one-time identities, and (3) monetizing one's own future behavior in a marketplace.

Keywords: Encryption, Decentralization, Fiduciaries, Surveillance Capitalism, Privacy

1. Privacy in the Age of Social Media

Facebook prompts its 2 billion users every day with a simple question, "What's on your mind?" This gentle nudge is the beginning of a rich funnel of engagement cues that remove the friction of privacy concerns from users and helps drive the company's $70 billion dollars of annual advertising revenues. Similarly, the flashing cursor inside of Google's search box conditions billions

Email addresses: seth@fiducia.care (S. Goldstein), pavel@fiducia.care (P. Machalek)

[1]Data Fiduciary Inc., Established 2019 in Mill Valley, CA

of users to share their most intimate intentions, generating more than $100 billion dollars a year in sales.

The immediate benefits of convenience often distract users from longer term privacy interests, and so Internet companies keep making it easier to engage with their algorithms: from Facebook Connect and Google oAuth to the emergence of intelligent assistants like Amazons Alexa and Apples Siri.

The slow and steady sublimation of privacy to convenience numbs us to its loss. Each data exposure leads to a death of a thousand cuts, and the constant stream of privacy breaches makes them seem inevitable. Facing Congress in February 2019, the CEO of Equifax refused to disclose his own date of birth and social security number, despite the fact that his company leaked such information for over 140 million Americans. Marriott, in plain text, lost identity and payment credentials for millions of guests. Outrage becomes neutered with each news cycle. Our increasing desensitization to the loss of privacy creates profound and pervasive emotional consequences.

In his 1968 essay, Westin describes a particular anxiety that results from the loss of these privacy rights:

> Knowledge or fear that one is under systematic observation in public places destroys the sense of relaxation and freedom that men seek in open spaces and public arenas. [1]

Almost fifty years later, Richards and Hartzog describe the same feeling:

> People feel confused and disempowered when it comes to their data. Instead of feeling confident that we will be protected when we share information with others, we increasingly feel helpless and resigned to our fate. [2]

Solove suggests that privacy comprises the following rights: 1) right to be left alone; 2) right to limited access to the self; 3) right to secrecy; 4) right to control of personal information; 5) right to person-hood and 6)right to intimacy [3].

The growth of smart phones, social apps, and AI puts individuals at a distinct disadvantage in terms of protecting their privacy. The lure of addictive "free" products such as the Facebook Newsfeed, Instagram Stories, or Google Search/Maps/Gmail blinds users to the hidden costs of these products: loss of privacy, loss of agency, loss of control over the means of personal data production.

Zuboff describes these costs further:

> Although some of these data are applied to product or service improvement, the rest are declared as a proprietary behavioral surplus, fed into advanced manufacturing processes known as machine intelligence, and fabricated into prediction products that anticipate what you will do now, soon, and later. Although the saying tells us If its free, then you are the product, that is also incorrect. We are the sources of surveillance capitalisms crucial surplus. Surveillance capitalisms actual customers are the enterprises that trade in its markets for future behavior. [4]

Engineers at social media and search companies develop addictive feedback loops through notifications and other dopamine-driving rewards [5]. The more engaging these apps are to users, the more personal data they are able to harvest. Companies have defended their history of user data extraction by suggesting that they have provided adequate notice and consent, and that their users are explicitly opting-in to share their personal data.

In fact, customers quickly scroll through privacy policies and click "I Understand."

> So, each and every Internet user, were they to read every privacy policy on every website they visit would spend 25 days out of the year just reading privacy policies! If it was your job to read privacy policies for 8 hours per day, it would take you 76 work days to complete the task. [6]

These asymmetric contracts reduce agency and are non-negotiable. Intermediaries like FB Connect and Google oAuth (which function like "fund of funds" in the allocation of consumer permissions to 3rd party apps) reinforce this inequality. Meanwhile, companies establish rich profiles of customers without these customers knowing what it known about them (for example, 74 percent of Facebook customers dont realize the site collects their interests to target ads.) [2]. This represents the growing challenge of *inverse privacy*:

> Due to progress in technology, institutions have become much better than you in recording data. As a result, shared data decays into inversely private. More inversely private information is produced when institutions analyze your private data. [7]

[2] http://www.pewinternet.org/2019/01/16/facebook-algorithms-and-personal-data/

The challenge therefore is that not only do companies have access to private user data, but they are far better at understanding this information than the "owners" of it are themselves.

2. The Problem of Surveillance Capitalism

Shoshanna Zuboff's work "The Age of Surveillance Capitalism" describes in depth the economic consequences of inverse privacy: the difference between what users know about themselves and what others know about them becomes a form of surplus value. She describes surveillance capitalism as

> A new economic order that claims human experience as free raw material for hidden commercial practices of extraction, prediction and sales.[8]

Given the technology infrastructure and cash reserves of the Internet monopolies, it is hard to imagine surveillance capitalism slowing anytime soon. How might the surplus value currently held by companies such as Facebook and Google be redistributed to users?

Surveillance capitalists sell probabilities of what users will do next. They sell historical data only to train AI systems to better predict *future* behavior. Their factories produce "free" social media, search, email and other services that attract user attention. Their business model process starts with *enabling* a user to do something easy (ie "what's on your mind?"), *anticipating* what they might do next (ie search auto-complete), then establishing predictive models for sale to marketers, which lead to more active behavioral modification such as *nudging*, *influencing* and ultimately *actuating* a commercial activity.

User experience engineers and growth hackers optimize onboarding flows and notification schemes to trigger bursts of dopamine that ease users down conversion funnels. As Hartzog testified before Congress' March 2019 hearing on "Policy Principles for a Federal Data Privacy Framework in the United States,"

> Companies create manipulative interfaces that exploit our built-in tendencies to prefer shiny, colorful buttons and ignore dull, grey ones. They may also shame us into feeling bad about withholding data or declining options. Many times, companies make the ability to exercise control possible but costly through forced

> work, subtle misdirection, and incentive tethering. Sometimes platforms design online services to wheedle people into oversharing, such as keeping a streak going or nudging people to share old posts or congratulate others on Facebook. Companies know how impulsive sharing can be and therefore implement an entire system is set up to make it so easy.

Privacy, however, is friction in this model: it is a monkey wrench wedged into the surveillance capitalist's funnel, one that users can hold onto so as not to fall into a pool of their own behavioral surplus. In his classic 1951 *Philosophical Investigations*, Wittgenstein defends the value of cognitive friction as essential to clear thinking:

> We have got on to slippery ice where there is no friction and so in a certain sense the conditions are ideal, but also, just because of that, we are unable to walk. We want to walk: so we need friction. Back to the rough ground! [9]

Back to the rough ground! is a rallying cry to counterbalance the relentless onset of surveillance capitalism. After years of promoting the reduction of friction for online businesses, it is now the re-establishment of friction that becomes paramount: such friction could come from regulators (who could mandate privacy by design), advertisers and researchers (who could stop purchasing dirty, conflicted data), surveillance capitalists themselves (who might be forced to make their sharing and search interfaces *less* persuasive), and people (who adopt strategies to shield themselves from surveillance).

In her recent paper "The Antitrust Case Against Facebook", Dana Srinivasan calls on empowering consumers with the ability to say no to surveillance in the form of a "Do Not Track switch":

> The fact that this centurys new communications utility is free but necessitates widespread surveillance of consumers is a paradox in a democracy. Facebook watches, monitors, and remembers what over 2 billion people do and say online. Contrary to what those in the advertising industry would have regulators think, American consumers value a state of no surveillance and have attempted to protect this aspect of their privacy since the beginning. The fact that the free market today offers no real alternative to this

> exchange is a reflection only of the failure of competition... For this, we need to empower consumers with a singular Do Not Track switch that can counter the collusion in the horizontal market. Consumers must be able to just say no to commercial surveillance. [10]

Whether it is a pervasive "NO" data sharing button that can be invoked across the Internet, or related tools to disguise future intentions, a new era of consumer data activism is necessary to teach people how to become less predictable to their technologies.

3. The Role of the Fiduciary

By disrupting the seamless sharing of their private information, users can recapture the value they create (which in aggregate drives the outsized profitability of surveillance capitalist businesses).

> People are not very good at privacy management; they do not understand the cumulative effects of their agreements to allow collection, analysis, use, and sale of information about them. [11]

Balkin introduces the concept of an Information Fiduciary as a mechanism to help people understand how their data is being used and manage their privacy without conflicts:

> Fiduciaries have two basic duties. The first is a duty of care. The fiduciary must take care to act competently and diligently so as not to harm the interests of the principal, beneficiary, or client. The second, and in many ways more important duty, is the duty of loyalty. Fiduciaries must keep their clients interests in mind and act in their clients interests... Because most professional relationships are fiduciary relationships, most professionals are also information fiduciaries. And that means, in particular, that professionals have duties to use the information they obtain about their clients for the clients benefit and not to use the information to the clients disadvantage. [11]

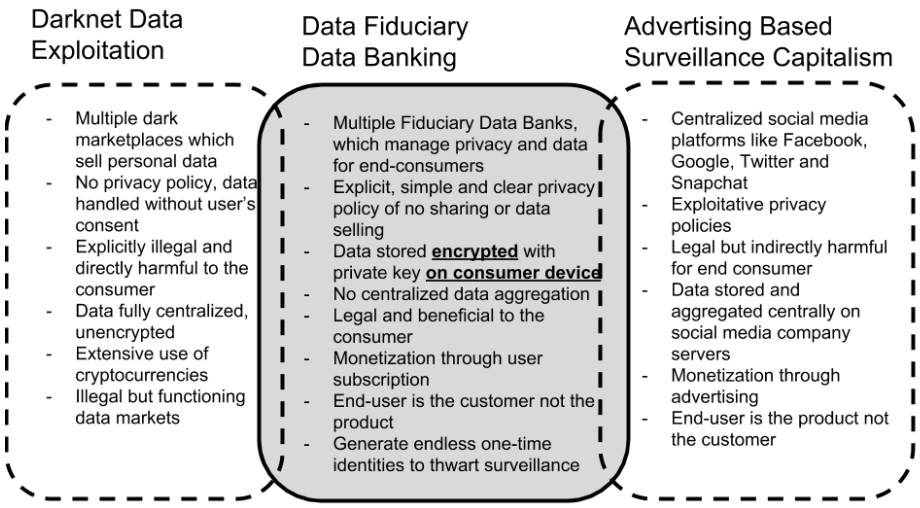
We define data fiduciaries here along the same lines as Richards and Hartzog, as "trustworthy data stewards that have four characteristics that

promote trust: they are honest, discreet, protective, and loyal." We also agree with much of Khan and Pozen's skepticism [12] about Balkin's belief that monopolist platforms like Facebook and Google can easily transition into trusted data fiduciaries for their users, since their business models of behavioral targeting and their prioritization of shareholder interests above user interests expose fundamental conflicts.

4. The Promise of Fiduciary Data Banks

Our solution calls for a new class of companies that emerge specifically and exclusively to serve as trusted data stewards. We refer to these companies as *Fiduciary Data Banks* (FDB). We see FDBs as serving a key role in the emerging data-centric world, where the structure of the relationship between the data emitter (e.g. Facebook), data fiduciary and the client (see Fig. 1) is modelled after the password managers of today and device-only wallets. For both the password manager and the wallet, the client holds the private keys to his other passwords and his crypto currency on his device. The private keys never leave the device and the software developer of the password manager and wallet never see the private keys (and neither can they help the customer recover lost private keys).

Figure 1: Data Bank schema, positioned between Surveillance Capitalism and the Dark Nets



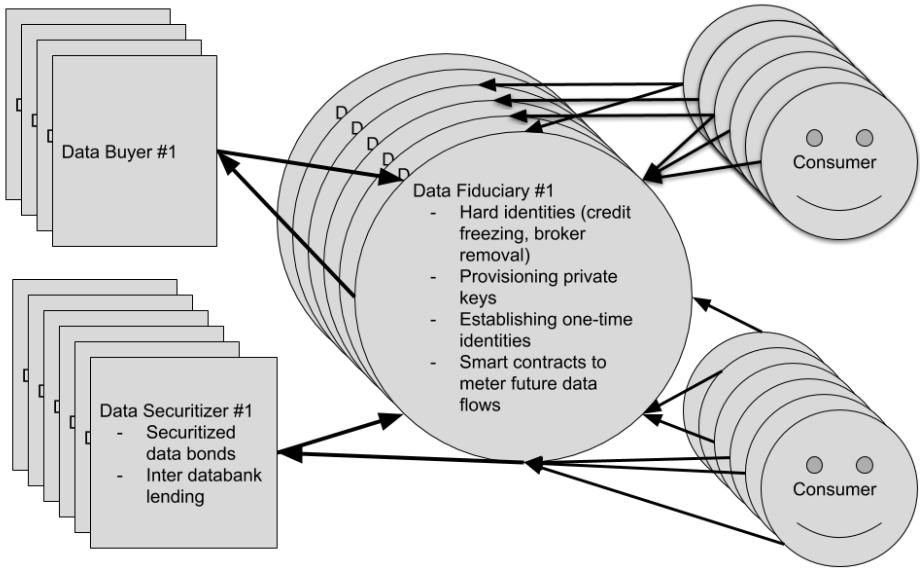
Fiduciary Data Banks help their clients defend their privacy rights from both surveillance capitalist platforms and illicit dark web sites by providing a variety of functions such as:

- **Profile**: Clients claim their official profile and restrict 3rd party access to it by deleting records from data brokers and freezing their credit with bureaus.
- **Private Key**: Clients establish a private key for their identity, and a BIP39[3] seed phrase as a form of backup.
- **Public Addresses**: Clients assume new one-time identities (name, email, mobile, debit card) for each interaction with a 3rd party.
- **Storage**: Secure encrypted storage for clients who wish to move their social media and search data off the servers of the surveillance capitalist platforms.
- **Statements**: Clients get real-time access to their current data holdings and market value where available.
- **Offers**: Clients receive offers from 3rd parties who wish to access their information.

When the customer has been using the FDB's services for a while, her credit file would have been frozen (preventing ID theft); furthermore, she will have been removed from online data brokers so that her information is unavailable for purchase on the Internet. By using one-time identities, she has left no new data trails for purchase by 3rd party data brokers. She has backed up her own social, search and email data on decentralized storage devices around the world to which she alone holds the private key (stored on her phone). Not even the FDB has access to the private key to unlock her personal data. After a period of time of practicing privacy hygiene with a reliable FDB, the customer has reduced and semi-anonymized her behavioral data such that even if leaks occur on centralized sites and end up for sale on the darknet, such details point to one-time emails, phones and debit cards that on their own do not reveal the customer's full ongoing data profile.

[3]https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki

Figure 2: Data Sharing and Securitization Framework facilitated by the Data Fiduciary



5. Data Asset Management

Once a sufficient level of data has been removed and pseudo-anonymity has been achieved (as described in the previous section), it will be up to the consumer to decide whether they want to monetize their data streams. The FDB will facilitate Data Sharing Agreements with 3rd parties on behalf of its clients within a framework depicted in Fig. 2. Customers will choose from among multiple FDBs to help them securitize their data flows with data buyers: *for example she might choose to sell a monthly subscription to her e-commerce transaction receipts as investment research to institutional investors via a smart contract directly mediated from her smartphone.*

A Data Promissory Exchange will connect people who wish to promise future access to their data with companies that want to guarantee such access. It will be based on a Data Metering Protocol that can verify that an individual has provided access to her data over a particular period. This will trigger a smart contract that issues tokens for validating data contributions, and provide a mechanism of exchange with companies who wish to purchase access to users.

This new model represents an alternative to Zuboff's analysis of surveillance capitalism, where companies like Google extract personal data from

customers to create surplus value sold to advertising customers in the form of behavioral futures contracts. In a Fiduciary Data Bank framework, the customer who generates personal data retains full agency in the marketplace.

6. The Problem of Data Inflation

One issue that impacts the value of personal data is the extent to which people use the same email address and mobile number to sign up for different services. Given the inverse privacy dynamics discussed earlier, companies are able to establish rich personal dossiers about individuals by correlating contact information with 3rd party databases. This produces surplus information about users regardless of whether data is required to accomplish a particular transaction. The propagation of personal data outside of one's immediate control creates a double spending problem: the value of one's data is inflated because it is available in so many different places (ie data promiscuity). To establish the highest price for one's future data stream, such information needs to be scarce. This suggests that people adopt a strategy of data monogamy in order to maximize the value of their information. Tokenizing identity through the use of private keys and one-time "burner" email addresses, telephone numbers and debit cards is our suggested strategy for maximizing the value of one's data.

7. Conclusions

We propose a new fiduciary data banking model that radically and aggressively retains consumer agency based on principles of encryption and local storage. Recent developments in the areas of public key cryptography, the blockchain and smart contracts offer useful approaches. Our solution encompasses (1) minimizing personal data exposure (2) managing one-time identities, and (3) monetizing one's own future behavior in a marketplace.

8. References

[1] A. F. Westin, Privacy and freedom, Washington and Lee Law Review 25 (1968) 166.

[2] N. Richards, W. Hartzog, Taking trust seriously in privacy law, Stan. Tech. L. Rev. 19 (2015) 431.

[3] D. J. Solove, Conceptualizing privacy, Cal. L. Rev. 90 (2002) 1087.

[4] S. Zuboff, Big other: surveillance capitalism and the prospects of an information civilization, Journal of Information Technology 30 (2015) 75–89.

[5] C. J. Hoofnagle, J. Whittington, Free: accounting for the costs of the internet's most popular price, UCLA L. Rev. 61 (2013) 606.

[6] A. Madrigal, Reading the privacy policies you encounter in a year would take 76 work days (2012).

[7] Y. Gurevich, E. Hudis, J. M. Wing, Inverse privacy, arXiv preprint arXiv:1510.03311 (2015).

[8] S. Zuboff, The Age of Surveillance Capitalism, Hachette, 2019.

[9] L. Wittgenstein, Philosophical investigations, John Wiley & Sons, 2009.

[10] D. Srinivasan, The antitrust case against facebook, Berkeley Business Law Journal 16 (2018).

[11] J. M. Balkin, Information fiduciaries and the first amendment, UCDL Rev. 49 (2015) 1183.

[12] L. Khan, D. Pozen, A skeptical view of information fiduciaries, Available at SSRN (2019).