

A Broken System

Over \$200 billion is spent on the acquisition and resale of personal identifiable information (PII) in the United States each year. The data is used to identify real-world people so that brands, agencies, and technology companies can sell, market, or target a specific demographic, an interest group, or characteristic of a person. For context, that is roughly equivalent to the gross domestic product (GDP) of New Zealand.

You might ask - where is this data coming from and how is it used? Why are you not in control of how, why, and where your data is used? Why are you not compensated?

Before we get into the solution, let's first define the problem. What is personally identifiable information (PII)?

PII is any data that can be used to identify you in the real world. This might be as obvious as your email address, social security number, a picture of you, or your home address. But may also be as sophisticated as identifying who are your friends and family, what you search for on the internet, or what you spend money on. It can be a single piece of information or a composition of information pieced together to identify you online.

This data is bought, sold, traded, and ransomed from large organizations, data resellers, and nefarious individuals/groups every day. It's the fuel of the internet - whole industries, from online advertising to social media, would collapse without a steady flow of data from its users and external sources.

Let's take a closer look at advertising: Organizations like Google, Facebook, and Twitter use your data—the topics you search for, the websites you visit, the topics you “like” on social media, the words

your write in your posts —to create a profile of your interests. As they learn more about you, they begin to understand what you're likely to buy, what you're likely to read, which people you may follow on social media. It's not a coincidence that the advertisements you see in social media, your email inbox, or on a website shows you products you may have looked at or bought recently. These companies are tracking everything you search for in order to advertise products that you are most likely to buy.

But what if you don't want your data used by these services? What if you want to control when and how your data is used? The truth is that there is no single option/method to "opt out" of how your data is used because control of your data is not centralized. There is no single group who has your data and is selling it - in fact, there are thousands of organizations who have copies of your data to utilize in their platforms or resell to other platforms at a premium.

And some individuals are aware of their data being used without their consent online. They create fake emails, remove/edit social media accounts, and slowly...slowly try to erase their PII from the internet. It's a laborious process that requires a dramatic change in the way they, and other modern internet-goers, leverage technology. These changes mean you can't take advantage of common social media tools, or pre-populate information in forms online, or even use mainstream technology like Google, Apple, or Microsoft products. So while removing your digital footprint is probably something that most people would like to do, it also makes it harder to use modern technology.

Unfortunately and perhaps inevitably, most people simply accept that they cannot control how their data is used so why go through the effort of removing their information online? Well, this is why we built Prime: we believe there's a better way.

A New Paradigm

Opting-In

The first step in controlling your data is to have the tools that enable you to choose when, how, and with whom you want to share your data. We call this 'opting-in.' By opting in, you agree to share the information with specific organizations for specific use cases.

Opting-in enables you to share your data with people and organizations that you approve. Not opting-in, means that data you have isn't shared with anyone - even Prime.

For example: What if you like having new products, like clothing or home goods, advertised to you by Google? Maybe you find it useful, like seeing new products, and you don't mind the ads in your sidebar. When Google requests your data, you can choose to share it with Google for their advertising of certain types of products. As your interests change, Google may request to use your new / updated data to better target products that may be of interest to you. At that point, you can opt-in to sharing again or opt-out.

Framework of Trust

Every system requires methods to regulate and monitor the health of the network. For Prime, we adopted three core tenants / proofs to guide us: Proof of Network, Proof of Humanity, and Proof of Intent. These proofs, and the underlying systems that support them are designed, to a) protect the integrity of you and your data and b) secure payment for the data you share.

Proof of Network: A system to indicate that you're not a bad actor by connecting to other trustworthy people in your network. The more connections you have the more our system trusts that you are who you say you are. People with high PoN scores earn token dividends from our network.

Proof of Humanity: A way to indicate that your identity, or at least the identity you want to sell, is tied to an actual human. You can choose to share some information, or no information, with our PoH proof. It's your choice. People with high PoH scores command higher values for their data in our marketplace.

Proof of Intent: A way to get indicate that you are willing to share sensitive information for the betterment of all people. The reality is that certain types of data, like healthcare data, is worth significantly more than other types of data. This is because that data is less common and filled with highly personal information that many people do not want to share. However, in the right hands, this data can also help humanity solve the hardest problems that we are facing today - like, it's cancer research. People with high PoI scores earn dividends, higher values, and multipliers for their information on Prime

- Dividends: Dividends are earned by maintaining sensitive data and having high PoN, PoH, and PoI scores

- Higher values: Higher demand means more money for that information.

- Multipliers: Multipliers are reserved for extremely sensitive and valuable information. By opting in to a multiplier data request, you will receive a multiple of the payment.

Storing and Sharing Information

One of the many problems with centralized data storage is that large databases become a target for hackers. The more user accounts that exist in a database, the more valuable it is for people who want access to your account data. Think of it like a bank account - if you wanted to break into a bank, would you target a bank or more or less money in it? More, of course!

The website Have I been Pwned estimates that there are over 11 billion stolen or leaked individual available on the internet today. For reference, there are nearly 8 billion people in the world, 4.66 billion of those people have internet, and 2.8 billion of them use Facebook.

Half a billion of those 11 billion accounts on HIBP are from a Facebook hack in April 2021.

So, how do you protect yourself? The only reasonable answer is to a) give complete control of ones data to that person, no one else. And b) decentralize data collection and storage. Instead of having a single database with thousands of accounts, you have one database with one account. Who controls access to that database? You, and only you.

An Open Marketplace

In a traditional marketplace transaction buyers exchange cash or other forms of currency for goods and services of equal value. The value of that good/service depends on what a business is selling, who it is selling to, where it is selling that product, etc. It's supply and demand - the greater the need for your product, the higher it sells for.

In our marketplace, sellers (individuals) of information securely and responsibly sell/exchange their data at their discretion. This means you, the owner of your data, gets to choose what data you would like to sell, how much you'd like to sell it for, who you would like to sell it to, and when you would like to sell it.

Buyers (organizations that acquire data) who are interested in your data can request information from you - it may be new or updated data. You can opt-in to share you data, or reject the request depending on what is being asked.

Buyers are evaluated under the same stringent guidelines for trust, data storage, and data use that sellers are. Each buyer is evaluated and scored on their relative strength in Proof of Network, Proof of Humanity, and Proof of Intent. Their relative scores on these Proofs are publicly available for all sellers prior to opting-in.

Furthermore, all transactions are stored on our blockchain on a public ledger. This means that any data request is registered on an immutable accounting of participants, value, and request details.

Our Platform

The Prime Blockchain

Our private blockchain (aka Primechain) maintains a record of every buyer and seller transaction in our system. Anytime a seller opts-in to a data request, and the request is fulfilled, the seller and buyer will be identified (cryptographic hash key) in the ledger. PII is never written to the Primechain.

Personal Data Vault

Each seller must use the Prime's mobile application to add, update, and store their data. Unless the seller opts-in to a data request, the data stored on their mobile device never leaves their mobile device. It is never stored on Prime's servers, never available to web services, and never shared with another seller. A seller's data is protected and secured in our personal data vault with 256 bit encryption, biometric signatures, a one-time paper key to retrieve lost data, and any security settings on the device.

Marketplace

Our marketplace is a open platform where data buyers request access to seller's data. The request comes in the form of a Request for Data (RFD) and defines what data they need, how they will use the data, and how long they will use the data will be used for. In addition, RFD's can contain a clause for data erasure/destruction after a certain period of time or set number of uses.

Prime serves as the arbiter of data requests and connects potential buyers with sellers who may be interested in opting-in to a data. All RFD's are purely optional opt-in requests. A seller is never forced to sell their data.