2015

Whitepaper

PRIVATE.ME AIMS TO MAKE PRIVACY POSSIBLE BY RETURNING CONTROL TO USERS AND PROVIDING FORGETFULNESS ACROSS THE INTERNET.

PRIVATE.ME WHITEPAPER

THE GROWING CONCERN OF PRIVACY

The role and scope of connectivity has grown incredibly since the birth of the Internet. From online dating to housing exchanges to professional networking, communities are becoming more and more intertwined and digitized. Simultaneously, as more and more online services arise, and more data gets collected and used by service providers, and thanks to technological advances, the cost of data storage for the companies collecting it, has decreased exponentially. Whereas in 1980 1GB of storage space cost $437,500, in 1990, $11,200, and in 2000, $11, today 1GB of storage costs only $.03[1]. The increase in connected services means that users are generating more data online and the rapidly shrinking cost of retaining it means more is being stored.

The information customers house with service providers often forms a part of that service. An online photo album would be meaningless if a user were unable or unwilling to transfer his or her files to the cloud. Likewise, some services are dramatically improved, or even made possible through analysis of user information. Relevant recommendations on shopping websites and radio stations that adapt to individuals' preferences deploy user data in a way that is often truly designed to benefit the consumer. But the massive amount of data that gets collected when people use online services also brings great risk.

When a business collects a user's data, it can use that data to make decisions based on customer information, including charging different prices to different people, or directing specific consumers toward more expensive options. Amazon[2] and Orbitz.com[3] were both caught engaging in these practices. Because user data is also valuable to businesses other than the ones that initially collect it, even the companies that do not exploit data themselves may sell it to aggregators or host advertising services that perform their own data collection and tracking. These massive piles of data can then follow users across platforms and services, ready to be used when a business finds use for them. The repositories of private data on service provider platforms also become appealing targets for hackers. Recent data breaches have wreaked havoc across industries including the recent hacks of Target, Lastpass, Ashley Madison, and the Heartbleed vulnerability that left countless websites exposed.

If user data is compromised through a hack or exploitation it can have real repercussions for both businesses and consumers. In 2014, companies that had data breaches had an average cost of $6.5 million associated with the breach[4]. A large portion of the cost was associated with loss of business due to lack of trust from consumers. Between 2009 and 2013, the percentage of Internet users who said they worry about the availability of information about them online rose from 33% to 50%, according to the

---

[1] http://www.statisticbrain.com/average-cost-of-hard-drive-storage/
[2] http://abcnews.go.com/Technology/story?id=119399&page=1
[3] online.wsj.com/news/articles/SB10001424052702304458604577488822667325882?mg=reno64-wsj&url=http%3A%2F%2Fonline.wsj.com%2Farticle%2FSB10001424052702304458604577488822667325882.html
[4] http://www-03.ibm.com/security/data-breach/

Pew Research Center[5]. Pew also reported that nearly 91% of adults feel they have lost control over how information is collected and used by companies[6]. 2014 also marked the 15th consecutive year in which identity theft was the number-one consumer complaint in the United States, according the Federal Trade Commission[7].

The need for online privacy has been present since the early days of the Internet, and it will continue to grow as our dependence on the Internet and the ability to process large amounts of data increases.

Private.me's Perspective on Privacy

Private.me believes that people have the right to control their own data and share it according to their own preferences. Private.me envisions a future where privacy is possible and consumers know exactly where their data is and retain the ability to revoke access after disclosing information. This is a future where 'deleted' means 'deleted,' not just invisible, and where hackers can't social engineer their way into large piles of data.

To achieve this, Private.me must fundamentally change the way information is handled online, starting with the relationship between service providers and their users.

Service providers are what make the Internet such an important part of modern life, and most providers do not have bad intentions regarding user data. However, the traditional operation of services includes packaging the storage of user data with the provision of a service. The challenge for consumers is that the companies that provide the best services in their industry do not necessarily also provide the best data storage or privacy policies as well, and, from the outside, it is difficult to evaluate how companies treat and handle data. By separating one from the other and providing users with a secure storage space that is under their own control, consumers are able to have cutting edge privacy and security while being free to interact with service providers as they please.

Private.me's Solution

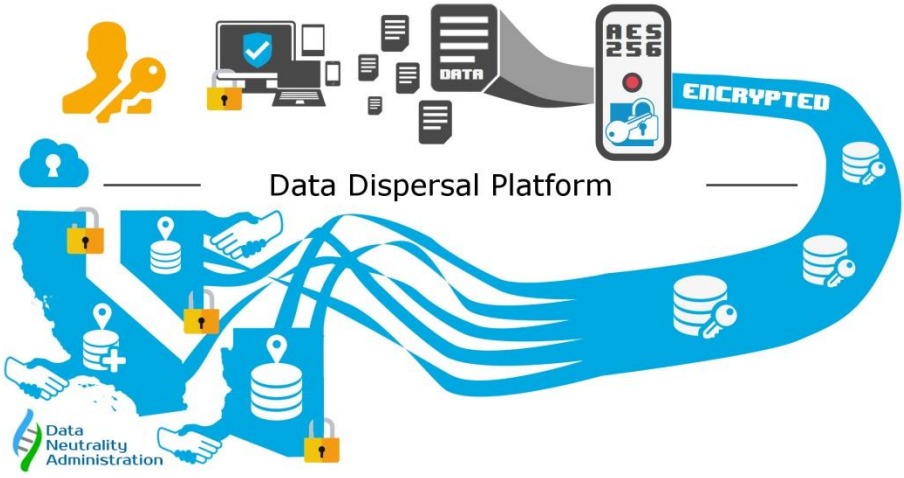
Private.me has created a secure and private storage space that, through a RESTful API, can be linked with almost any Software as a Service (SaaS) provider to allow users to engage with the SaaS while retaining control over their data. This system encrypts and disperses data to a network of vaults managed by nonprofits. This allows data to be securely stored in servers that are independently managed by organizations that have no profit motive.

Data Dispersal Platform

The Data Dispersal Platform (DDP) is Private.me's method of securely and privately storing user data. The DDP uses sophisticated, well-established, algorithms to encrypt with AES-256 keys, fragment data, and then distribute the fragments to geographically scattered storage nodes on a series of dispersed networks. No complete copy of the original data exists on any single node anywhere in the network. Encrypted, fragmented, distributed across multiple networks, and with access controlled by users rather

[5] pewinternet.org/files/old-media//Files/Reports/2013/PIP_AnonymityOnline_090513.pdf
[6] http://www.pewinternet.org/files/2014/11/PI_PublicPerceptionsofPrivacy_111214.pdf
[7] https://www.ftc.gov/news-events/press-releases/2015/02/identity-theft-tops-ftcs-consumer-complaint-categories-again-2014

than service providers, the DDP-protected data is nothing but useless bits until it is pulled together and decrypted to make readable information.



Components Gatekeeper

The gatekeeper maintains the credentials required to access the Platform, and screens all transactions. Once the Gatekeeper has authenticated the identity and authorization level of a service requesting a transaction, it provides the requester with the credentials necessary to complete the transaction with the Platform. Private.me has built and maintains the Gatekeeper in accordance with a rigorous Secure Software Development Life Cycle (SSDLC), and, for hosting, leverages hardened high-security servers in facilities subscribing to SSAE-16.

Platform

The Platform performs the encryption and decryption, fragmenting and reuniting, and distribution and recall of user information. Once the Gatekeeper authorizes a transaction, the relevant information passes between the Platform and the service provider. After the completion of a transaction, the Platform and the service provider's systems delete the information after it is sent to the storage nodes.

Storage Nodes

The encrypted and fragmented personal data resides in geographically separate locations on separate networks. Were hackers to gain access to even several of these nodes and succeed in downloading and decrypting the information belonging to a user, which is virtually impossible, they still would only have fragmented information. Readable information is only achieved when the data has been correctly reassembled by the Platform. The storage nodes are under the management of the Data Neutrality Administration (DNA).

Data Neutrality Administration

The DNA manages a network of nonprofit data-storage locations, all of which are independent, geographically dispersed, and established as mutual benefit corporations under the laws of California. The DNA is set up with strict bylaws and regulations governing the access and use of any data stored on their servers. Their bylaws forbid the nonprofits from sharing, either among themselves, with other member nonprofits, or with third parties, information that is stored on their servers, unless authorized by the

owners of that information. Additionally, each member of the nonprofits' board of directors bears the fiduciary responsibility of safeguarding users' information. The board's governing responsibilities are not only collective; individual board members are bound by the legal obligations of protection, loyalty, and obedience. Federal law enjoins the board to ensure that no inappropriate private exposure occurs that might result in individuals who can influence the affairs of the nonprofit to control organizational assets.

The use of nonprofits is a proprietary innovation that allows established security and encryption solutions to be under the control of users instead of corporations. In addition, under a traditional organizational structure data dispersal would not be as strong a protection against hackers as within the company at least one person would normally have administrative rights or access to all servers. The incorporation of independent nonprofits eliminates those types of concerns.

User Interaction

User interaction with Private.me is designed to be easy, secure and to provide them with control over their own data. As part of this, users sign on to other service providers through Private.me's secure Single Sign On (SSO) in order to authenticate their authority over the data. When they would like to review or modify permissions, or to delete data generated through their interactions with any of the SaaSes with whom they use Private.me to store data, users can do so through a control panel on Private.me. The control panel is only accessible to users, not SaaSes, as it is the users who decide the permissions.

Secure Single Sign On

Secure SSO allows users to engage with new companies with confidence as they are able to have the ease of SSO and a rigorous security standard. The Private.me approach to SSO evolved from the OpenAuth 2.0 (OAuth2) specification, and gained further hardening of key steps and components. It differs from OAuth2 in the following ways:

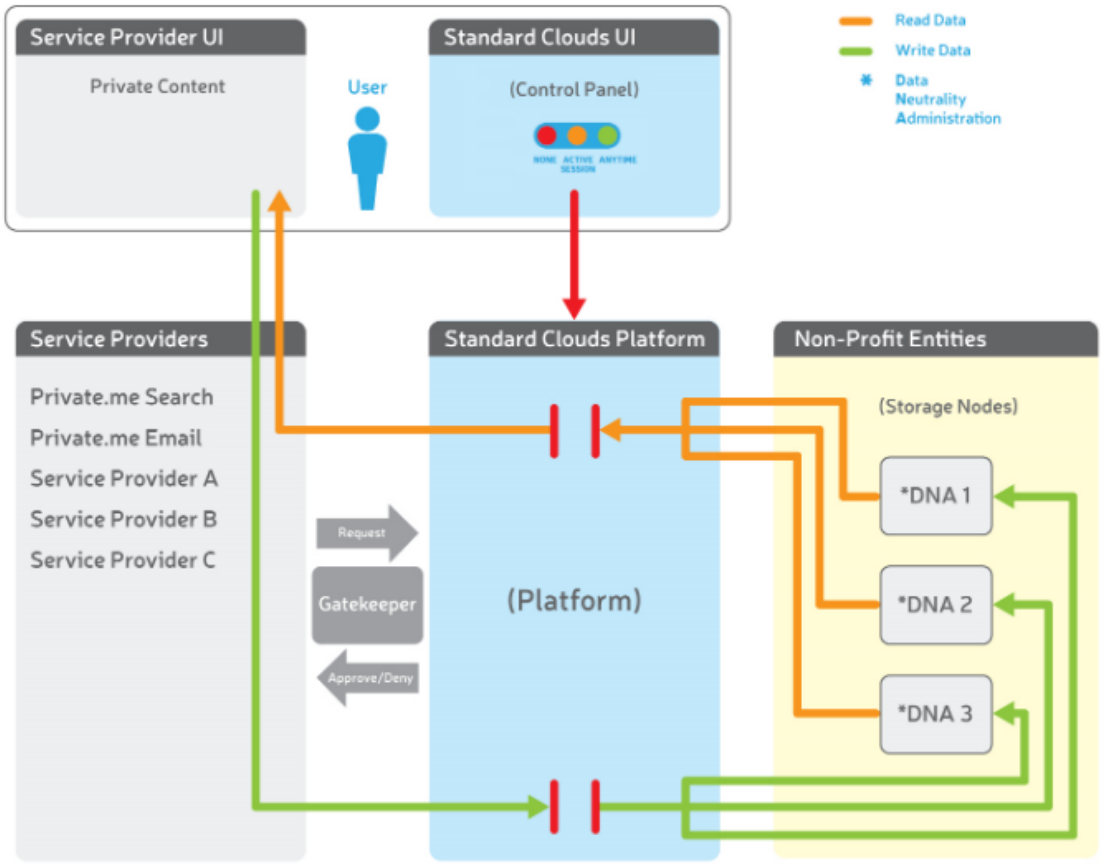
- In OAuth2, the authorization code passes through the web browser, but Private.me sends authenticated user information and the secure access token by an out of band channel directly to a partner endpoint. In bypassing the user's web browser and encouraging partner sites to keep private information on the back end web server and database, Private.me rules out an entire class of vulnerabilities.
- OAuth2 requires two calls in sequence for this type of delegated authentication sequence: first acquiring an authorization code, and then acquiring a secure access token. This is done to avoid sending the token through the web browser. Since Private.me has eliminated that vulnerability already, only one step is needed.
- OAuth2 relies heavily on TLS for assurance of security, arguably leaving it open to malicious certificates and man-in-the-middle attacks. Private.me also uses TLS, but further requires the partner to sign each request cryptographically to provide a higher level of protection.

Authentication Flow

Control Panel

The Private.me control panel is where users can delete their data and/or decide when the SaaSes they use can have access to it. Users are given the choice between always allowing access, providing access when they are logged in, or never providing access. When the toggle is set to never provide access, however, users might find that some SaaSes cannot be used as their data is required to provide the service. The

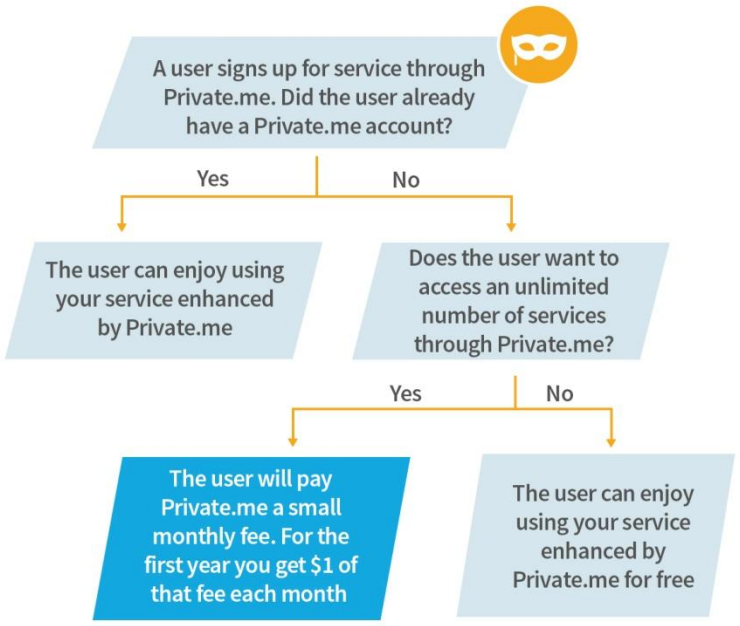
Gatekeeper uses the settings on the control panel to help decide whether or not to grant a SaaS access to the user's data.



Monetization

Private.me operates with a freemium business model where users are able to try Private.me's services at no charge in order to establish the value. All of Private.me's current services are free, but once Private.me has established enough value for users it will offer the use of a set number of services/connections to SaaSes for free and charge users a small monthly fee to connect their storage space to all other services available on the Private.me platform. Private.me will also provide a certain amount of storage space for free, and will charge on a sliding scale for increased storage use. Because Private.me recovers the cost of storage from its clients, storage of data costs nothing for the SaaSes and can be a way to reduce the total cost of ownership of data storage.

As a 'thank you' to SaaSes that draw users to Private.me, Private.me offers a revenue share opportunity. If a user opts to sign up for a SaaS through Private.me but does not already have an account, he or she is presented with an opportunity to create a Private.me account. If an account created through a SaaS later subscribes for access to all of the services available through Private.me then Private.me offers the SaaS $1/month for the first year.



Implications for Privacy

Private.me's solution for data storage has a profound impact on privacy and security and greatly increases the ease of interaction between users and service providers.

Users

By engaging with companies through the Private.me platform, users gain an obvious advantage when it comes to privacy. They regain control over their own data and can feel confident that their data is secured in a safe manner. This reduces the uncertainty that often comes with using a new service or company as, when using Private.me for data storage, users can automatically understand how their data will be treated even with unfamiliar services or companies.

Existing consumer-focused privacy solutions tend to address the generation of a trail of data, but Private.me focuses instead on the data users want to generate. When an exchange of data between a customer and a service provider is necessary for a service, control over the privacy and care of that data has always been in the hands of the SaaS. Private.me changes this model completely, for the first time making it possible for those who care most about the data to take ownership of it.

Service Providers

Service providers also benefit from the increased privacy offered by this solution. Traditionally, SaaSes were responsible for securing user data and thus were also required to persuade potential customers that they would be good stewards of that data. Private.me relieves SaaSes of that burden by providing users with access to a system where they do not have to establish trust with the SaaS.

The increased security, both with the secure SSO and the DDP also reduces the risk of data or account hijacking from hackers. Hacking can result in harm to business reputations and can have significant

repercussions to profits. In addition to this risk being decreased overall, it is also transferred away from the SaaS, as it is Private.me, not the SaaS, which contracts with users to securely store their data.

Conclusion

Private.me's solution for handling data addresses both the vulnerability of databases to hackers as well as the mistrust users can have in service providers. It secures data in a way that does not interfere with the normal functioning of services, so that an option for privacy can truly exist. Now that the technology is in place, it is time to take a stand for privacy.