Where's My Data?
DATA TRANSPARENCY

Information Fiduciary Consortium: A United Front

"Data is the new oil" is an often used phrase that aims to underscore the weight of how much data now fuels our information economy. Consumers hand over incredibly personal data in exchange for free services, often without realizing what the true implications of that deal entails. Understandably, companies have business models to follow and must compete in their markets. However, now more than ever – particularly with the recent move by Congress to roll back user privacy rules for ISPs – we are at a breaking point. There needs to be change.

Corporations have an opportunity to proactively reassure their users that they take an interest in their users' privacy.

To that end, companies and academia are working to create the Information Fiduciary Consortium (IFC), a consortium that will work to find a balance between corporate and public interest. This ensures corporations can continue to use consumer data to fuel their businesses, while mitigating the toxic side effects of poor data management practices.

Companies who join the IFC agree (1) to pursue self-regulation, (2) to follow a standards-based approach to industry best practices, and (3) to proactively seek innovation-friendly legislation.

1) Self-regulation: IFC companies in good faith and varying degrees will have committed to fair security and privacy practices around user data collection, analysis, use, disclosure, and sale. We have built a basic prototype to demonstrate a possible technical solution where a user could log on to wheresmydata.org and view the pathway of his/her data.
2) Standards-based approach: In the industry currently, compliance regimes are used between companies to prove that they are behaving correctly to one-another. We would like to create a parallel regime that companies can use to prove to regular consumers that they are handling their data properly.

3) Innovation-friendly legislation: In return, the Consortium will advocate for federal legislation to provide a safe harbor to member companies from lawsuits and burdensome requirements imposed by the patchwork of state regulations related to user data protection, disclosure penalties, and data handling requirements. Just as a united front of technology companies has received substantial goodwill through public pushes for anti-surveillance legislation and net neutrality, the technology brands should come together once again and advocate for user privacy.

Benefits of Joining the IFC

- **Stand out.** In an expanding world of online services and technologies, companies that join the IFC can proudly declare—and actively show—that they take privacy seriously.
- **Build user trust.** Surveys show that privacy is a critical factor for consumers when choosing new products and services. Joining the IFC will help build a brand that your users can trust will treat them with respect while still offering something amazing.
- **Innovate without the fear of a lawsuit.** When companies can agree to take steps to protect user privacy knowing that they will be protected from lawsuits and local regulations, innovation will flourish. The IFC will push to protect companies through nationwide regulation that rewards proactive privacy practices.

We Want Your Help

The IFC imagines a future where companies can prosper and users can be assured their privacy interests are secure. To build this future, we need your help. Members of the Harvard Berkman Klein Center and Yale Law's Information Society Project will convene at the Berkman Klein Center in the Fall of 2017 and we want you to have a seat at the table in these conversations. We have compiled a list of suggestions for a tier based approach to the IFC and look forward to your feedback. If you are interested in learning more about getting involved with the Consortium—or simply have a question or a piece of feedback—please contact us at feedback@wheresmydata.org.

Requirements to Join the IFC

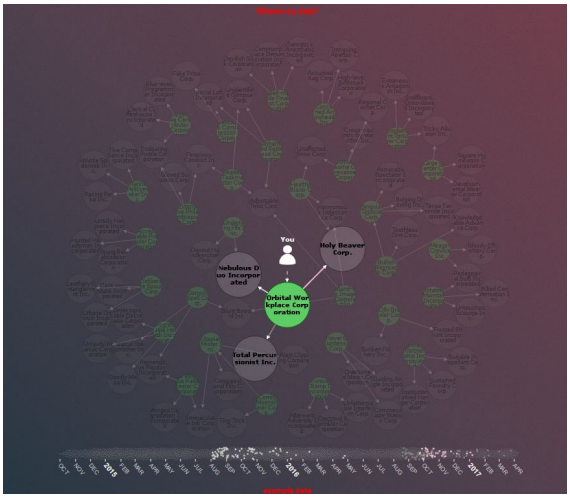
We acknowledge that not all companies will be able to address all the outlined requirements and with that in mind we suggest the following tiered approach:

- Tier A: (the initial level)
    - **Security:** Companies will perform regular security audits and disclose any data breaches to affected customers. Companies will commit to implement a specified level of technical and organizational measures to protect data.
- Tier AA: (the next, more developed level)
    - **Transparency:** Companies will maintain an audit log of any user data shared with other companies or entities. Companies will also publish data storage information and clarify what happens to user data if acquired or bankrupt.
    - **Portability:** Companies will provide users with the ability to export their data in a usable format, as well as allow for the ability to completely close an account.
- Tier AAA: (an advanced level)
    - **Community:** Companies agree to share or sell user data, individually or in aggregate, with other Consortium companies that have agreed to similar rules as outlined by the Consortium agreement.
    - **User authorization**: Sharing or selling data should entirely be based on the consent and purpose agreed upon with the client
    - **Neutrality:** Companies will enable users to experience features without any personalization.
    - **Deletion**: Companies will actively have the ability to destroy any collected information on the user upon request.

Technical Implementation

For the IFC to be successful, *consumers* need to understand the value they are getting out of a company participating. This is what differentiates the IFC from other security compliance regimes – it is about directly providing value to consumers in a way that they can understand, which builds trust in the company's brand from the consumer's standpoint.

This means that the Consortium cannot just be a set of guidelines and rules, but also an interactive system that consumers can use. We must combine technology with process to make a strong impression.



Centering around the duty of ***transparency***, we've built an interactive visualization tool that consumers can use to see:

1. *who* is being transparent about data sharing, and
2. *where* their data goes.

By making small, 1-line changes to programs, companies can report a "share" – including (a) what company is the data going to, (b) whose data is included, (c) where a user can go to learn more about the share.

This data, stored in a distributed database across participating companies, can be accessed by consumers to see their personal data. Each share is associated with an identifier (such as an email address), and as long as a user can prove they own the identifier (for example, in the case of email address, by following a link emailed to them), they can see the shares associated with it over time.

A beacon of hope: EU data privacy standards

To aid in understanding of the current state of user data protection in the European Union, we might want to consider the IFC as the US alternative to the EU-US Privacy Shield Framework. The EU-US Privacy Shield Framework allows US based companies to self-certify for compliance to EU data privacy regulations – joining itself is voluntary, but once eligible the critical features are as follows:

- Informing individuals about data processing
- Maintaining data integrity and limiting scope of usage
- Ensuring accountability for data transferred to third parties
- Transparency related to law enforcement actions.

It can be enforced under US law through private compliance mechanisms as well as federal regulatory bodies, such as the Federal Trade Commission. The IFC could be a valid alternative to companies that might not want to fully adopt EU-US Privacy Shield rules but are willing to voluntarily apply some rules - offered with the different tiers of the framework to show they are taking customers' data privacy concerns seriously. It provides an avenue for companies to show they are taking customers' data privacy concerns seriously.

In contrast to US data privacy law, personal data belongs to the affected individual in Europe and not to the organization who is collecting, storing or analyzing data. As an example, the following are two fundamental rights that have been established in Germany:

- Since 1983, data collection and the purpose of data processing must be authorized by the individual
- Since 2008, the right to have personal data protected.

Their main objective is the protection of individuals against misuse of their personal data. To achieve this goal data protection and data privacy is a fundamental right - unlike in the US.

The European General Data Protection Regulation (GDPR), soon to be law across the EU, gives consumers the following rights:

- the right to data portability
- the right to erasure
- assurance that there is compliance with legal obligations in data processing

- privacy by design
- consent
- reporting of data breaches.

Conclusion

On the internet, we are our data. Who owns it? Who controls it? An oil rush is underway to collect as much data about users as possible. But we need to think about more than just the quarterly reports. We need to build for generations to come.

Corporations and users can both benefit from the still-nascent data economy. That requires corporations to collect data with user consent, use it and store it responsibly, and share it with user's knowledge.

The data economy is only sustainable with user trust. Trust begins with transparency.

Data Transparency.

Have a question or a piece of feedback?

Please contact us at feedback@wheresmydata.org.