

This is Google's cache of <https://www.hackerleague.org/hackathons/data-privacy-legal-hackathon/hacks/clearbutton-personal-data-notice-registry>. It is a snapshot of the page as it appeared on Jan 20, 2016 20:20:32 GMT.

The **current page** could have changed in the meantime. [Learn more](#)

Full version [Text-only version](#) [View source](#)

Tip: To quickly find your search term on this page, press **Ctrl+F** or **⌘-F** (Mac) and use the find bar.

Toggle navigation

 [Logo](#)  [Logo-only](#)

- [Hackathons](#)
- [Hacks](#)

- [Sign Up](#)
- [Sign In](#)



- [Overview](#)
- [Announcements](#)
- [Projects](#)
- [Participants](#)
- [More](#)
 - [Resources](#)
 - [Rules](#)
 - [Schedule](#)
 - [Themes](#)

ClearButton Personal Data Notice Registry

In Progress

Favorites (3)

What is ClearButton?

The modern economy is **fueled by personal data**. People have a valid expectation - and sometime a legal right - to know who has what data personal data about them.

Today, there is no way to discover or request this information about you from all who have it.

[ClearButton](#) initiative is developing an open source, open standards and open architecture approach to address this need with a Personal Data Notice Registry.

Registering to Signal Request for Notice Solves Several Problems at Once

Envisioned broadly along the lines of a Do Not Call registry, but for the purpose of enabling individuals to request notice from those who hold personal data about them. Organizations that participate in the registry service would use ClearButton to send links for personal data disclosures to individuals registered as requesting such notice.

Consider that the Fair Information Practices generally and corresponding legal regimes such as the EU Privacy Directive, the US Federal Privacy Act of 1974 and state statutes such as the Massachusetts Fair Information Practices Act (MGL Ch66A) are all triggered when a person makes a request to an entity holding their personal data. While it is plausible to make such a request in a targeted manner to a given entity, or even a handful of entities, it is currently impractical to the point of impossibility for any individual to discover all entities holding personal data about them and to accomplish a request to each of them. Yet, this is the very first and most fundamental step in regaining and maintaining individual control and transparency about their own personal data.

The act of signing up to a Do Not Call registry legally signals a request under the applicable rules that the individual has put telemarketers on notice they should be removed from covered types of marketing lists. The insight behind ClearButton is that a corollary service for posing requests for Personal Data is needed. Furthermore, applying Web 2.0 OAuth2 enabled and REST-based approaches favored by the openPDS team of the MIT Media Lab's Human Dynamics group, such a registry service set could be accomplished in vastly more efficient, effective, convenient, secure, robust, resilient and flexible ways than prior architectures have allowed.

Who Can Access the Links and What Data Is Linked to?

The links should be accessible only by individuals holding a valid corresponding account with the registry. Metadata describing personal information or data sets it hold by the disclosing party would be available via the notice links. To the maximum extent practicable,

organizations participating would also support buttons enabling registered individuals to directly download or export the underlying personal data. Like BlueButtonPlus and Green Button, the role of ClearButton would be a universal button for the download of any type of personal data when available, and minimally for receiving notice of disclosure of the existence of personal data by those who hold it.

Why Bother? Who Cares? You Gonna Make Me?

Structuring such a registry system and accompanying services such that each key stakeholder achieves more value by participating than not participating is a key design requirement. While in theory a statute or regulation requiring uniform new rights to personal data would accomplish the same purposes, it is postulated that an integrated business, legal and technical architecture along the lines outlined above can afford enough value to enough parties at each phase so that all participation would be totally voluntary and self-propelling through proof of concept, prototype, pilot, beta, initial operation, and iterative expansion and beyond. Coercive law has it's place, to be sure, but the vantage point of the New Deal on Data is that the personal data fueled digital economy is attractive enough to earn it's own way without the need to force engagement.

In short, everybody can make more money, reduce risks and have a fun time using the ClearButton approach... we think...

The purpose of traveling to NYC and participating in this Data Privacy Legal Hackathon is to test the hypothesis by focusing time, energy and attention on hacking together a horizontal prototype expressing an initial complete statement of the functions, flows, roles, relationships, components, services and key use cases of the concept. And to collaborate with others who have innovative and compatible ideas or who wish to contribute to developing the ClearButton concept.

Demo Video



Comments



[View Website](#) [View Demo](#)

Team



[nicole](#)

Nicole Sharer



[eCitizen](#)

Dazza Greenwood



[eLKay](#)

Lina Kaisey



[DantheMan](#)

Dan Nelson



- [About](#)
- [Organizer Feedback](#)
- [Blog](#)

- Copyright © 2014 Hacker League
- |
- [Terms of Use](#)
- |
- [Privacy Policy](#)

- Hacker League is a production of **Intel Corporation**

-
-
-
-

[Close](#)

Sign In

Email

Password

[Forgot password?](#)
No account yet?

[Sign Up](#)

Sign In

[Cancel](#)