No Safe Haven: The Storage of Data Secrets

Harry Halpin (W3C/MIT) hhalpin@w3.org

Given the aftermath of the shutdown of Snowden's e-mail provider Lavabit, where can one safely store encrypted data? In other words, By "safe", one means a location for servers that will be resistant to both physical seizure and legal compulsion to reveal any secrets, where secrets are ideally client encrypted and not simply passwords managed by the server (as in the case of Lavabit). While Lavabit both offered to hand over Snowden's email and was nearly forced by hand over all users' email, it seems not unreasonable to imagine an email provider that is neither legally or physically capable of revealing user secrets. However, despite the crypto-libertarian dreams of a cryptographically safe server farms, there is no clear safe jurisdiction.

First, we'll draw up in detail a list of requirements for a data safe haven, including practical aspects such as the availability of fibre as well as requirements on the data and the stability of the country's regime. Then we'll overview a number of jurisdictions and dispel a number of myths about supposed data safe havens such as Iceland and Hong Kong. While the Data Protection act helps, Europe fairs poorly due to the Data Retention Act. Lastly, we'll present a technical solution that creates a 'floating safe haven' that attempts to minimize risk by storing the data across multiple jurisdictions.