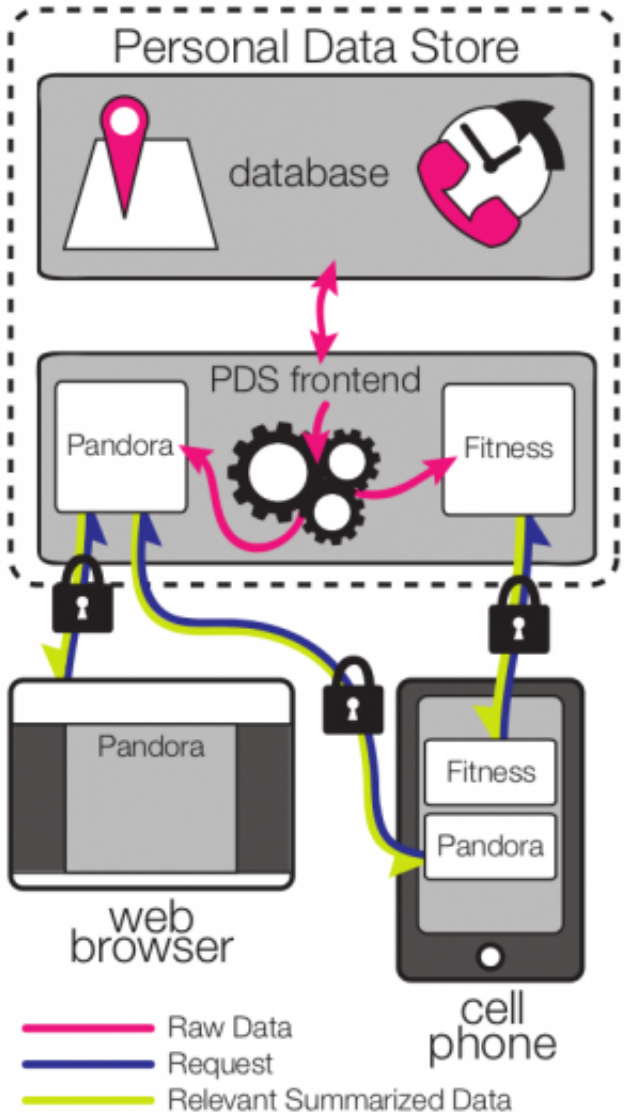
openPDS software focuses on control of personal data

7 October 2013, by Nancy Owano



(Phys.org) —Regarded as a building block for the personal data ecosystem, open PDS has arrived. As Thomas Hardjono, technical lead of the MIT Consortium for Kerberos and Internet Trust commented in *New Scientist*, "We want people to have equitable access to their data. Today, AT&T and Verizon have access to my GPS data, but I don't."

If you want to install an app on your smartphone, openPDS sits in between the app requester and you, controlling the flow of information that will be released back to the app requester. Hosted either on a smartphone or on an Internet-connected hard drive, it siphons off data from the phone or computer but the software allows users greater control of how the data is used and shared.

OpenPDS was developed at the MIT Media Lab and ID3 (Institute for Data Driven Design, a research and educational group in Boston). "Open" in openPDS suggests its open source nature and PDS stands for Personal Data Store. The idea is for a computer user to have one place where all the data resides, a store that gives the user greater control over what kinds of data he or she wants to share with any third party requesting information.

Yves-Alexandre de Montjoye, who participated in the MIT Media Lab undertaking, posed the question on his own page, "In a world where sensors, data storage and processing power are too cheap to meter how do you ensure that users can realize the full value of their data while protecting their privacy?"

openPDS, as the user's data store, answers questions from external applications or services with answers that the user allows. Computations on user data are performed in the safe environment of the PDS, under the control of the user. Only answers in the form of summarized data necessary to the app leaves the boundaries of the user's PDS. Said deMontjoye: "The dimensionality of the data can be reduced on-the-fly to certified answers before being anonymously shared."

Rather than exporting raw accelerometer or GPS data, it could be sufficient for an app to know if you are active or which geographic zone you are in. A question such as "Do you spend time in London?"

could be only a yes or no reply.

The stated core principles of openPDS are: Answers, not Data; Permissions for Sharing; Auditability; and Governance.

According to a paper on the software, openPDS is implemented with related Trust Network services. (The MIT Human Dynamics Lab developed a Trust Network communication architecture that "ensures that this new data driven society is secure and fair.")

The Funf open sensing framework is used to collect sensor data on Android phones, securely uploading the data sets to OpenPDS. (The Funf Open Sensing Framework is for mobile devices, supported and maintained by Behavio. The idea is to provide an open source, reusable set of functionalities, enabling the collection, uploading, and configuration of a range of data signals accessible via mobile phones.) Software is provided on an open source basis, under the LGPL license. The modules are available on Github.

More information:
www.demontjoye.com/projects.html
idcubed.org/wp-content/uploads … m-Human-Dynamics.pdf
openpds.media.mit.edu/
www.newscientist.com/article/m … you-and-the-nsa.html

APA citation: openPDS software focuses on control of personal data (2013, October 7) retrieved 27 October 2021 from https://phys.org/news/2013-10-openpds-software-focuses-personal.html