Personal Information Controller Service (PICS)

Marco Winckler[1](✉), Laurent Goncalves[2], Olivier Nicolas[2], Frédérique Biennier[3], Hind Benfenatki[3], Thierry Despeyroux[4], Nourhène Alaya[4], Alex Deslée[5], Mbaye Fall Diallo[5], Isabelle Collin-Lachaud[5], Gautier Ubersfeld[6], and Christophe Cianchi[7]

[1] Université Nice Sophia Antipolis, Nice, France
winckler@unice.fr
[2] Softeam, Toulouse, France
{lgoncalves,onicolas}@e-citiz.com
[3] LIRIS, INSA Lyon, Lyon, France
[4] Inria, Le Chesnay, France
[5] Université de Lille, Lille, France
[6] Anyware Service, Labège, France
[7] Business Card Associates, Paris, France

Abstract. This paper presents a view at glance of the project PICS (which stands for Personal Information Controller Service) that is concerned by personal data protection. More specifically we present a software platform that allows users to control the exchanges between Web-based Personal Information Management Systems (the so-called PIMS that store users' personal data) and SaaS services (such as e-commerce applications) using a reinforced authentication. The ultimate goal of this platform is to empower users by allowing them to have full control on personal data exchange. Moreover, the platform includes specific components to help users to solve cognitive demanding tasks related to the data protection such as how to properly interpret Terms of Service (ToS) imposed by the SaaS, recall previous users interactions with the SaaS (ex. personal data exchanged with the SaaS and the corresponding term of services), and detect unauthorized use of personal data. The technical solution proposed by PICS is a suitable implementation of the General Data Protection Regulation (GDPR). We present the motivations, challenges and research questions that lead to the technical solution proposed by PICS.

Keywords: Personal data protection · Personal information systems · GDPR

1 Towards User-Centric Data Protection

It is a terribly thing to think that personal data is being collected without user's consent for that a simple answer to privacy problems would be to maximally inform the users about how much data was being kept and sold about them. Personal data protection has been a long concern in many countries like France but only more recently it has been regulated by the means of the European General Data Protection Regulation (GDPR) [3] forcing many companies to adjust their data handling processes, consent forms, and

M. Bakaev et al. (Eds.): ICWE 2019, LNCS 11496, pp. 530–533, 2019.
https://doi.org/10.1007/978-3-030-19274-7_40

privacy policies to comply with the GDPR's transparency requirements. The basic premise for the GDPR is that users must be informed about the use made of their personal data [1]. Notifying users about a system's data practices is supposed to enable users to make informed privacy decisions and yet, current notice and choice mechanisms, such as public policies and Terms of Service (ToS), are often ineffective because they are neither usable nor useful, and are therefore ignored by users [2]. Whilst the GDPR tries to regulate the use of personal data, it also creates two cognitive demanding tasks to the users: (i) how to analyze ToS, and (ii) how to remember huge amount of personal data that the SaaS is authorized to store.

Nowadays, users store many personal data in Web applications (such as Dropbox, Google drive, Linkedin, Facebook, etc.) that act as Personal Information Data Management Systems (PIMS) [4]. Connecting PIMS and SaaS offer two advantages: on one hand it is a suitable solution for delivering personal data to the SaaS; on the other hand, the PIMS can store ToS and recall users of whom possess his personal data. The interoperability between PIMS and SaaS (such as e-commerce Web sites) is not a technical problem per se but a security failure on one service might increase the risk of data disclosure of other services [5].

It important to recall that according to the GDPR, data protection relies on a promise of use of personal data for a specific purpose, defined by a ToS. However, if users suspect that a SaaS violates the agreement, the number of complaints can quickly increase given that the rest of the procedure has to be done by service providers who might have juridical and IT divisions overbooked of request of clarification.

In order to solve these problems, we have created a consortium of researchers and industrialists that came up with a software platform called PICS (Personal Information Controller Service), which is eponym of the project. The rest of this paper present the overall architecture of this platform and illustrate the prototype. The last section summarizes the underlying research questions and the future work.

2 Overall Architecture of PICS

The overall architecture of the PICS platform is illustrated by Fig. 1. As we shall see, PICS mediates all the user interaction with third-party services that might contain (or require) personal data from the users, this includes both the SaaS and the PIMS. This mediation is meant to promote data protection and prevent that a security failure of a SaaS would affect the PIMS (and vice-versa). The security of PICS is enhanced by strong authentication mechanisms featuring a combination of user login plus physical authentication via a wearable device (such as an electronic bracelet). PICS is made of three core modules, as follows:

- The *personal data controller* is the central piece that connects all the other components. It includes a user interface allowing users to connect to third-party services (PIMS or Saas) and mediate the transfer of personal data between them. It is important to say that the PICS itself does not store any personal data. For that, users should identify a data storage (such as Google drive, Dropbox, Linkedin, etc.) that will act as a PIMS for recording all personal data, ToS and transactions made between the PIMS and SaaS.

- The *ToS analyzer* is a specialized tool that is able to process a ToS provided by a SaaS and codify the terms of ToS according to a specialized Ontology that covers all the dimensions of personal data protection referred by the GRDP [6]. The results of *ToS analyzer* are accessible to the users via the *personal data controller* by the means of a visual language as illustrated by Fig. 2.
- The *data mining traces of use* is a very specialized tool which is able to perform advanced search over the Web to discover traces of uses of personal data. This tool allow users to check where their personal data is available to SaaS. The results are shown at the *personal data controller*.

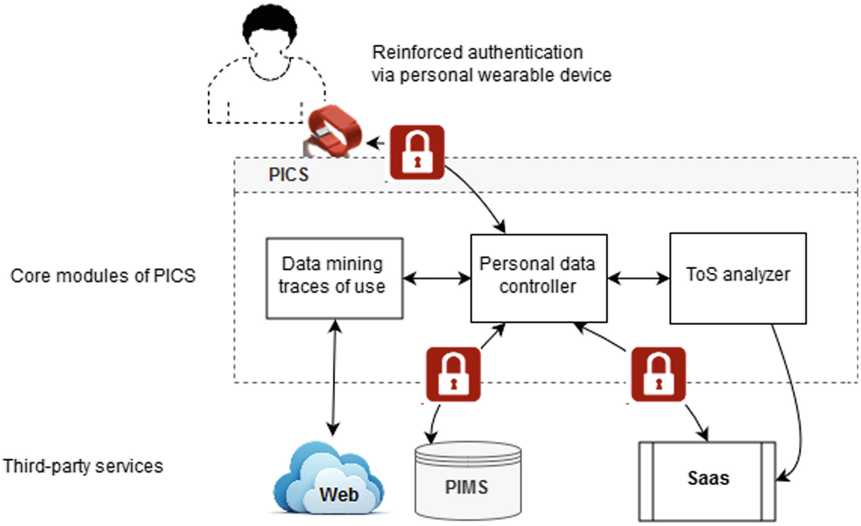
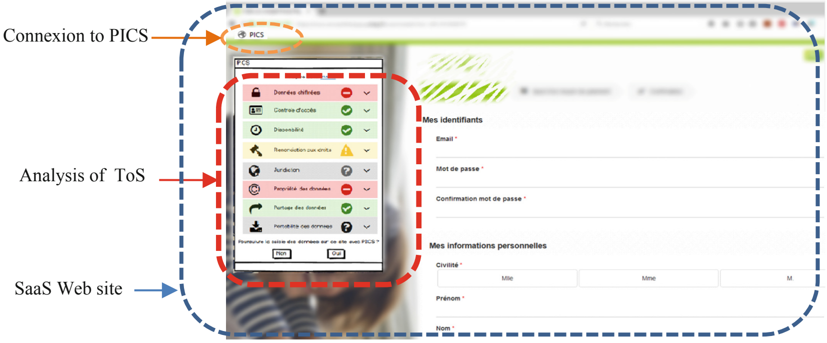


Fig. 1. Overall architecture of PICS



PICS

Données chiffrées
Controle d'accès
Disponibilité
Renonciation aux droits
Juridiction
Propriété des données
Partage des données
Portabilité des données

Poursuivre la saisie des données sur ce site avec PICS ?

Non Oui

Mes identifiants

Email *

Mot de passe *

Confirmation mot de passe *

Mes informations personnelles

Civilité *

Mlle Mme M

Prénom *

Nom *

Fig. 2. A view at glance of PICS featuring the analysis of Terms of Service of SaaS. (Color figure online)

3 Tool Support

The PICS architecture was implemented featuring a Web plugin as illustrated by Fig. 2. Once installed in the browser, the PICS menu appears in the tool bar allowing the user to access to all features supported by the PICS core modules. When the users connect to the PICS for the first time, he must register a login plus a physical wearable device that will be asked to identify the user in the future. Every time the user connects to the PICS it must provide the login plus the wearable device which communicate with PICS via a FIDO interface [7]. Figure 2 illustrates a scenario where after visiting a SaaS Web site, the user use the PICS menu to triggers the analysis of ToS. The results of such as an analysis is shown as a floating window featuring a list of GRDP dimensions. The icons, the keywords and color coding (green/red/gray/yellow) are meant to provide the users with a quick synthesis of the ToS.

4 Research Questions and Future Work

The project PICS raise many research questions. First, how to formalize the dimensions (such as duration of storage, location of the storage, data ownership…) recognized by the GDPR? That led us to the development of an Ontology [6] for processing ToS. The second question was how to secure the access to the data so that sensible personal data is not easily stolen by cracking a password? For that, we have investigated the use of wearable devices to reinforce the authentication. Another question is which architecture would prevent accidental personal data disclosure? We have proposed two complementary solutions: first, an independent module that does not store any data but mediate the data transfer between the PIMS and SaaS; second, a specialized data-mining tool for discovery of the use of personal data over the Web. Currently we have a proof of concept that demonstrates the feasibility of our ideas and an advanced prototype for demonstrations. Our on-going work includes the testing of the prototype with end-users to identify the potential adoption of the solution.

References

1. Lazar, J., Stein, M.A.: Disability, Human Rights, and Information Technology, 1st edn. University of Pennsylvania Press, Philadelphia (2017)
2. Terms of Service - didn't read. https://tosdr.org/. Accessed 25 Mar 2019
3. GDPR. https://eur-lex.europa.eu/eli/reg/2016/679/oj. Accessed 25 Mar 2019
4. Firmenich, S., Gaits, V., Gordillo, S., Rossi, G., Winckler, M.: Supporting users tasks with personal information management and web forms augmentation. In: Brambilla, M., Tokuda, T., Tolksdorf, R. (eds.) ICWE 2012. LNCS, vol. 7387, pp. 268–282. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-31753-8_20
5. Schaub, F., Balebako, R., Durity, A., Cranor, L.: A design space for effective privacy notices. In: SOUPS 2015, pp. 1–17. USENIX Association, Berkeley (2015)
6. Benfenatki, H., Biennier, F., Winckler, M., Goncalves, L., Nicolas, O., Saoud, Z.: Towards a User Centric Personal Data Protection Framework. http://chi-gdpr.webflow.io/. Accessed 25 Mar 2019
7. FIDO Alliance. https://fidoalliance.org/. Accessed 25 Mar 2019