SHORT TERM SCIENTIFIC MISSION (STSM) SCIENTIFIC REPORT

This report is submitted for approval by the STSM applicant to the STSM coordinator

Action number: CA16105
STSM title:Towards formal, computable privacy requirements
STSM start and end date: 25/02/2019 to 03/08/2019
Grantee name: Alain Couillault

PURPOSE OF THE STSM:

Our approach is to foster ethics by design by crossing technical and ethical requirements even before writing the first line of code. General Data Protection Regulation (GDPR) compliance is a major concern for the targetted enet collect CALL platform. All the more so as it need to be balanced with both training and research efficiency. A previous STSM was dedicated to extending the P3P former W3C standard with requirements from the GDPR. The purpose of the Short Term Scientific Mission is to confront these two approaches and try to implement the GDPR/P3P compliant taxonomy into an executable privacy policy language.

DESCRIPTION OF WORK CARRIED OUT DURING THE STSMS

The STSM occured between February 19th and March 1st 2019 at the NTUA and involved a team composed of
• Sofia Almpani, National Technical University of Athens
• Alain Couillault, Apoliade
• Maria Gavriilidou, ILSP / Athena RC
• Dimitri Kouzapas, National Technical University of Athens
• Penny Labropoulou, ILSP / Athena RC
• Thodoris Mitsikas, National Technical University of Athens
• Alexandros Nousias, NCSR ”DEMOKRITOS”, MyData Global Network, Advanced Quality Services Ltd
• Petros Stefaneas, National Technical University of Athens

The team met three times a week to exchange on the question raised. The work initialized during the STMS will be pursued after this two week session to result in a common article meant for publication. During these two weeks, we collaborated to work on a formal way to describe privacy notices and terms of use, and to render them in a easily readable way to the users, ie in the form of logos.

Funded by the Horizon 2020 Framework Programme
of the European Union

DESCRIPTION OF THE MAIN RESULTS OBTAINED

The issue of the readibily of online agreements has been raised for decades.
For example [Jensen and Potts, 2004] noticed that only 6% of the 64 privacy policies they examined are ‘accessible to the 28.3% of the Internet population with less than or equal to a high school education’. More recently, Choice Australia published a video which shows that the reading of Amazon Kindle’s terms and condition take 8 hours and 55 minutes [1] . This issue is getting more important with the enforcement of the General Data Protection Regulation (GDPR) which is based on the users’ so-called informed consent. Several attempts have been made to approach this issue of easy access to online agreements [Couillault, 2018], including the Plateform for Privacy Preferences (P3P) former W3C standard. The main idea of the P3P is to define a formal way for companies to describe their online agreements, and publish them in a computer readable format. According to [Cranor, 2012], this approach faced the companies’ unwillingness to play the game.
Our approach is different and relies on the crowd to transform online privacy notices into a formal description from which logos can be displaid to the user. This requires to define a formal enough representation of the online agreements, prepare the environment for the crowdsourced annotation, and infering logos from this annotation. The MAUDE environment [Pitsiladis and Stefaneas, 2018] is seen as providing some background for the formalization of online agreements.
During this STSM, we defined the several steps to associate online agreements into a set of logos:

- Define the set of logos, by examining existing approaches
- Defining logo set (actually, defining the meaning of the logos).
- Defining an annotation guide for the crowdsourced annotation
- infering logos from the annotation
- identifiying a set of online agreements for the experiment
- Conducting an annotation of by the crowd
- Evaluation the results

FUTURE COLLABORATIONS (if applicable)

We expect to present the results of the experiment in an international conference, worshop or publication related to formal and legal issues.

A) BIBLIOGRAPHY

[Couillault, 2018] Couillault, A. (2018). Enet collect short term scientific mission report. Technical report, Apoliade.
[Cranor, 2012] Cranor, L. F. (2012). Necessary but not sufficient: Standardized mechanisms for privacy notice and choice. Journal of Telecommunications and High Technology Law,, 10(2).
[Jensen and Potts, 2004] Jensen, C. and Potts, C. (2004). Privacy policies as decision-making tools: An evaluation of online privacy notices. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI ’04, pages 471–478, New York, NY, USA. ACM.
[Pitsiladis and Stefaneas, 2018] Pitsiladis, G. V. and Stefaneas, P. (2018). Implementation of privacy calculus and its type checking in maude. In Margaria,T. and Steffen, B., editors, Leveraging Applications of Formal Methods, Verification and Validation. Verification, pages 477–493, Cham. Springer International Publishing.