

Compliance Traceability: Privacy Policies as Software Development Artifacts

Sebastian Zimmeck¹, Peter Story², Rafael Goldstein¹, David Baraka¹, Shaoyan Li², Yuanyuan Feng², and Norman Sadeh²

¹ Department of Mathematics and Computer Science, Wesleyan University
{szimmeck,rgoldstein01,dbaraka}@wesleyan.edu

² School of Computer Science, Carnegie Mellon University

{pstory,shaoyan1,yuanyua2}@andrew.cmu.edu, sadeh@cs.cmu.edu

Abstract. The increasing importance of data privacy is met by legislators around the world with new privacy laws. However, it was shown that many developers struggle to understand the privacy implications of their code and the law they have to adhere to. Commercially available privacy policy generators are intended to help developers to properly disclose their privacy practices by guiding them through a questionnaire and generating a privacy policy based on the answers to the presented questions. However, state-of-the-art generators are inherently limited by the error-prone nature of the questionnaire-based approach. They are necessarily reliant on developers' ability to answer questions on their programs' functionality accurately as well as their timeliness in updating their answers in order to reflect software changes.

We propose to mitigate the potential for compliance issues by leveraging code analysis for purposes of generating privacy policies. We design and implement a policy generator for iOS apps written in Swift that uses three resources: (1) templates with standard language that every policy must include to be compliant with legal provisions, for example, the General Data Protection Regulation (GDPR), (2) policy snippets generated from an app's source code analysis, and (3) developer input via a wizard-based user interface. We think that privacy transparency can be increased and compliance issues reduced by establishing policy generation as a native extension of the software development process. Ultimately, the integration of policy generation into the software development process enables the traceability of compliance requirements originating from new privacy laws and the evolving regulatory landscape.

Keywords: privacy · compliance · privacy policies · static analysis · mobile applications · software development · iOS

Our approach is to integrate privacy analysis and policy generation in three stages: template provisioning, code analysis, and wizard fine tuning. Figure 1 shows an overview of our approach as well as a sample analysis result from our implementation.

