Towards Usable Privacy Policies: Semi-automatically Extracting Data Practices From Websites' Privacy Policies

Norman Sadeh[1]*, Alessandro Acquisti[1], Travis D. Breaux[1], Lorrie Faith Cranor[1], Aleecia M. McDonald[2], Joel Reidenberg[3], Noah A. Smith[1], Fei Liu[1], N. Cameron Russell[3], Florian Schaub[1], Shomir Wilson[1], James T. Graves[1], Pedro Giovanni Leon[1], Rohan Ramanath[1], Ashwini Rao[1]

[1]Carnegie Mellon University
Pittsburgh, PA 15213

[2]Stanford University
Stanford, CA 94305

[3]Fordham University
New York, NY 10023

1. MOTIVATION

Natural language privacy policies have become the de facto standard to address "notice and choice" on the Web. However, users generally do not read these policies and those who do struggle to understand them. Initiatives to overcome this problem with machine readable privacy policies or other solutions that require website operators to adhere to more stringent requirements have run into obstacles, with website operators showing reluctance to commit to anything more than what they currently do.

In this presentation, we will summarize major results of work conducted over the past two years in the context of the "Usable Privacy Policy Project", a large National Science Foundation Frontier project that combines machine learning (ML), natural language processing (NLP) and crowdsourcing to semi-automatically annotate privacy policies. The project also builds models of issues that people are least likely to be aware of and most likely to care about to focus the annotation process and design plug-ins with succinct and intuitive summaries of privacy policies. Further details about this project are available at www.usableprivacy.org including a comprehensive list of publications. Time permitting, we also propose to briefly demonstrate some of our annotations tools and resources we plan to release prior to PrivCon 2016.

2. APPROACH OVERVIEW

Research on user preference modeling suggests that a small number of key features in privacy policies largely determines whether users are comfortable interacting with a website and what information they feel comfortable disclosing as part of their interaction [3, 6]. This may include particular types of sensitive information collected by a site as well as the purpose for such collection (e.g., with which third parties this information is shared and for what particular purpose). Over the past two years, our project has experimented with different types of crowdsourcing frameworks, including different ways of subdividing crowdsourcing tasks, different ways of supporting crowdworkers. We have evaluated the reliability of different categories of crowdworkers, looking in particular at agreements both within and across different such categories. And we have also experimented with different ways of deploying machine learning and natural language processing techniques to semi-automate the annotation process and increase the productivity of crowdworkers. Concurrently, we have developed models of issues that people are most likely to care about in different contexts (e.g., different categories of websites) as well as models of what people believe different websites do and what they least expect websites to do with their data. These models are in turn used to prioritize the annotation process and develop browser plug-ins intended to highlight information that is most likely to help users without overwhelming them with details they are unlikely to care about. A third part of this project focuses on the analysis of privacy policies, including looking at the ambiguity of the language and statements found in privacy policies as well as comparing privacy policies across different sectors and their evolution over time.

2.1 Semi-automated Privacy Policy Feature Extraction

We extract relevant features from privacy policies in a hybrid approach that combines crowdsourcing, machine learning and NLP. We leverage crowdsourcing to obtain annotations of privacy policies in terms of what information is collected by a website, whether that information is shared with third parties with or without the user's consent, and whether the collected data can be deleted by users.

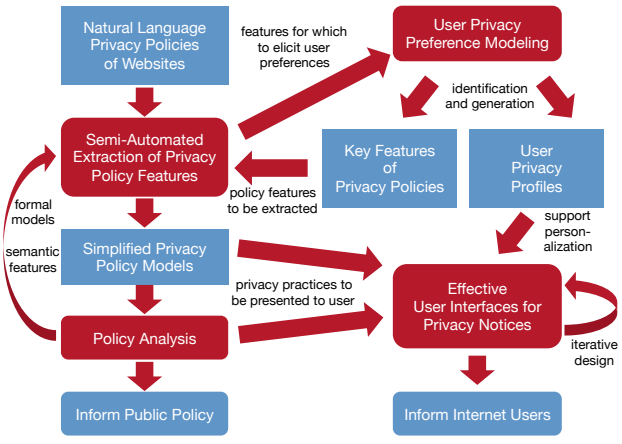

Figure 1: Overview of the proposed approach.

Ensuring that crowdsourcing yields high quality data requires careful task design. Encouraged by our prior results [2], we are experimenting with different task decomposition approaches to enhance annotation quality. Those approaches cover general data practices, such as collection, processing, or sharing with third

* Point of contact: Norman Sadeh (sadeh@cs.cmu.edu)

parties; different information types, such as contact information, current location, or financial information; as well as more fine-grained annotations of recipients of information and purpose statements [4, 5].

The resulting annotation are used to generate NLP and ML models. For instance, we employ sequence alignment to identify policy segments that likely pertain to the same data practice across different policies [10]. We currently leverage the NLP results to improve annotation interfaces for our crowdsourcing effort and optimizing task scheduling, e.g., by selecting or highlighting parts of the policy, which are potentially relevant for a specific annotation question.

2.2 Privacy Policy Analysis

We use salient information extracted from privacy policies to reason about the website's data practices and conduct extensive privacy policy analysis for multiple purposes. Translating policy features into descriptive logic statements facilitates detection of inconsistencies and contradictions in privacy policies [4]. Annotation disagreement among crowd workers further helps identifying potential ambiguities in the policy. Comparing a website's privacy policy with those from similar websites holds the potential to detect likely omissions in the privacy policy. Temporal monitoring of changes in privacy policies facilitates content-based trend analysis. We use policy analysis results to provide more effective and accurate privacy notices to users. Furthermore, we combine reasoning results with legal analysis of privacy policies to study the effectiveness of self-regulation efforts in different sectors and inform public policy. In addition, we plan to make analysis results available to website operators in order to help them improve their privacy policies.

2.3 Privacy Preference Modeling

A major objective is to make privacy policies more usable and accessible to website users. Thus, an important aspect of our work is the identification of those aspects of privacy policies that are most relevant to users. These models can be used to focus the extraction of privacy policy features as well as the development of more effective privacy notices. This work ha resolved around a series of user studies looking at privacy concerns expectations, and preferences, for example, in relation to online behavioral advertising [7]. Another dimension of this work involved developing a better understanding of cognitive biases that may negatively affect individuals' privacy decisions. We hope in turn to use this insight to further enhance our privacy plug-ins [1].

Part of this work has involved crowdsourcing and machine learning to collect users' privacy preferences at scale in and develop privacy preference profiles that can be used to developed personalized privacy notices [8].

2.4 Effective Privacy User Interfaces

As part of this presentation, we will showcase designs of some new privacy plug-ins and discuss results of a study aimed at evaluating and comparing their merits.

3. SUMMARY

This presentation will provide an overview of a large-scale multi-disciplinary effort aimed at semi-automatically extracting privacy policy annotations. This work, which has been going on for a little over two years, has already produced a number of results and techniques. They range from machine learning, crowdsourcing and natural language processing techniques to user privacy preference and expectation models that can be used to simplify the presentation of privacy policies to users. Time permitting, we propose to also demo some of the tools developed by our project and discuss their implications on the future of notice and choice and on the analysis of privacy policies by organizations such as the FTC.

Acknowledgments

This work is supported by the National Science Foundation under Grant No. CNS 13-30596.

4. REFERENCES

[1] A. Acquisti. Nudging privacy: The behavioral economics of personal information. *IEEE Security & Privacy*, 7(6):82–85, 2009.

[2] W. Ammar, S. Wilson, N. Sadeh, and N. A. Smith. Automatic categorization of privacy policies: A pilot study. Tech report CMU-ISR-12-114, 2012.

[3] M. Benisch, P. G. Kelley, N. Sadeh, and L. F. Cranor. Capturing location-privacy preferences: quantifying accuracy and user-burden tradeoffs. *Personal and Ubiquitous Computing*, 15(7):679–694, Oct. 2011.

[4] T. D. Breaux, H. Hibshi, and A. Rao. Eddy, a formal language for specifying and analyzing data flow specifications for conflicting privacy requirements. *Requirements Engineering*, pages 1–27, 2013.

[5] T. D. Breaux and F. Schaub. Scaling Requirements Extraction to the Crowd: Experiments with Privacy Policies. In Proc. RE ’14. IEEE, 2014.

[6] P. G. Kelley, J. Bresee, L. F. Cranor, and R. W. Reeder. A ”Nutrition label” for privacy. In *Proc. SOUPS ’09*. ACM, 2009.

[7] P. G. Leon, B. Ur, Y. Wang, M. Sleeper, R. Balebako, R. Shay, L. Bauer, M. Christodorescu, and L. F. Cranor. What matters to users?: Factors that affect users’ willingness to share information with online advertisers. In *Proc. SOUPS ’13*. ACM, 2013.

[8] B. Liu, J. Lin, and N. Sadeh. Reconciling mobile app privacy and usability on smartphones: Could user privacy profiles help? In *Proc. WWW ’14*. ACM, 2014.

[9] A. M. McDonald and L. F. Cranor. The cost of reading privacy policies. *I/S: A Journal of Law and Policy for the Information Society*, 4(3):543–568, 2008.

[10] R. Ramanath, F. Liu, N. Sadeh, and N. A. Smith. Unsupervised alignment of privacy policies using hidden Markov models. In *Proc. ACL ’14*, 2014.