Rating Indicator Criteria for Privacy Policies

Joel R. Reidenberg
Stanley D. and Nikki Waxberg Chair and Professor of Law, Fordham Law School
150 W. 62nd Street
New York, NY 10023
jreidenberg@law.fordham.edu

N. Cameron Russell
Executive Director, Fordham CLIP
150 W. 62nd Street
New York, NY 10023
nrussell2@law.fordham.edu

Thomas B. Norton
Privacy Fellow, Fordham CLIP
150 W. 62nd Street
New York, NY 10023
tnorton1@law.fordham.edu

1. INTRODUCTION

This short paper describes ongoing research to identify the legal and policy criteria necessary for the development of meaningful privacy rating indicators. Previous and current attempts to provide online privacy rating indicators such as grades and nutrition labels thus far have had only limited success and have not been widely adopted. The purpose of this research is to review the history of online privacy rating indicators, to identify deficiencies and obstacles to meaningful ratings, and to map the requirements or criteria that need to be established in law and policy for indicators to be meaningful and successful.

2. REVIEWING THE HISTORY OF ONLINE PRIVACY INDICATORS

2.1 Prior Attempts

Privacy policies are notoriously complex and not meaningful for users. Various attempts have tried to synthesize the content of privacy policies into specific indicators such as grades, scores, nutrition labels or certifications. The research identifies prior and current attempts to create rating indicators that are more meaningful for users than the complex policies.

The key examples of privacy grades or scores are:

- ToS:DR [1]
- PrivacyGrade,org [2]

The key examples of privacy labeling are:

- Privacy Bird [3]
- EU General Data Protection Regulation standardized privacy icons [4]
- Moms With Apps (MWA) Badge [5]
- Nutrition labels [6]
- Mozilla icon [7]
- ESRB icon [8]
- Disconnect.me [9]

The key examples of privacy certification seals are:

- TRUSTe [10]
- Better Business Bureau seal [11]

These indicators, however, have not gained widespread traction across the web for reasons including business and consumer acceptance of rating criteria, rating accuracy, reliability, and sustainability.

2.2 Goals for Privacy Indicators

The research explores the past and current attempts and shows that these efforts to develop indicators seek to achieve three common objectives and goals: 1) to provide consumers with more meaningful notice; 2) to empower consumers; and 3) to nudge data processors to improve their privacy notices.

3. RATING DEFICIENCIES AND OBSTACLES

The analysis of the various attempts to develop rating indicators shows specific deficiencies and obstacles for the effectiveness of any rating indicator.

3.1 Scoring Criteria

Scoring criteria can suffer from selection and weighting deficiencies. The selection of metrics for scoring embeds subjectivity and there is a general lack of standardization. Likewise, the weighting of elements in the scoring criteria is subjective and often does not account for the contextual complexity of data practices. For example, are collection, sharing, use, and retention data practices all included within the scoring criteria? Should collection practices and sharing practices be weighted equally? Should all sharing practices be equally weighted or are some sharing practices less privacy friendly than others?

Symposium on Usable Privacy and Security (SOUPS) 2016, June 22-24, 2016, Denver, Colorado.

3.2 Accurate Interpretation

There are also numerous issues relating to accurate interpretation of privacy statements. For example, one study of icons to represent behavioral advertising practices found that representations were confusing and concluded that it was unclear how well online behavioral advertising could actually communicate with users. [12] Policy language is often ambiguous and vague and, notwithstanding, reasonable minds can differ on contextual interpretation. [13] When users annotate privacy policies, both the questions asked and the answers provided may inject ambiguity. [13] Privacy policies often serve to carve out legal rights rather than describe real data practices with granularity and nuance. Policies are often silent on particular data practices, which may cause confusion to Internet users failing to account for a legal default that treats silence as permissive, not prohibitive, with respect to a certain data practice.

3.3 Reliability of Rating Agent

Issues also arise with the reliability of the rating agent. Specifically, the integrity of the rating agent and the agent's fidelity to the rating criteria may be important obstacles. As an example, during the past few years, privacy seal companies have been publicly criticized for deceptive practices. [14] Similarly, the consistency of the rating agent and the visibility of the rating provider are often problematic because of the plethora of niche agents.

3.4 Sustainability

The sustainability of rating systems is frequently deficient. Rating indicators are often dependent on single organizations without long term incentives or resources to continue. For instance, the promising Mozilla icon project stalled when its initiator left Mozilla to cofound a healthcare startup.

4. MAPPING LAW AND POLICY FOR A WORKABLE APPROACH

The research analysis will seek to map the law and policy needs for more meaningful, adoptable rating indicators. The researchers will suggest that, in order for privacy rating indicators to work, rating mechanisms must convey to users what a privacy policy says with respect to recognized criteria rather than an interpretation of meaning. This allows the website user to individually determine how criteria are weighted and interpreted. In addition, rating mechanisms cannot successfully convey what policies "mean" in many instances because of the inherent legal ambiguity of those policies.

Alternatively, the rating criteria will need a recognized consensus that is most likely to come from public adoption of legal rules or policies. Rating indicators must also align with legal canons of contract interpretation and legal defaults of silence. Rating systems must further have a means to verify the fidelity of the ratings to the criteria. Moreover, rating systems must reduce any ambiguity in questions presented to annotators because privacy policy language will be replete with ambiguity and vagueness. [15] The researchers will also suggest that providing ranges of agreement as to interpretation of language, rather than definitive conclusions made by the provider of the rating, reduces subjectivity and shifts inevitable interpretative issues to individual users and to the market.

5. ACKNOWLEDGMENTS

Fordham CLIP Project Fellows Antoine Bon, Sam Borenzweig, Tim Carter, Elle Davis, and Stephanie Tallering provided research support for this study. Grant CNS-1330214 from the National Science Foundation to the Center on Law and Information Policy at the Fordham University School of Law, New York, NY (Fordham CLIP) and a Fordham Faculty Fellowship supported work on this study.

.

[1] Terms of Service; Didn't Read, https://tosdr.org/ (last visited July 4, 2015).

[2] Privacy Grade, http://privacygrade.org/faq.

[3] Privacy Bird, http://www.privacybird.org/.

[4] General Data Protection Regulation, Art. 12(7), http://www.europarl.europa.eu/news/en/news-room/20160407IPR21776/Data-protection-reform-Parliament-approves-new-rules-fit-for-the-digital-era.

[5] Know What's Inside, https://momswithapps.com/discover.

[6] Kelly, P, Bressee, J. and Cranor, L., A "Nutrition" Label for Privacy, SOUPS (2009) http://cups.cs.cmu.edu/soups/2009/proceedings/a4-kelley.pdf.

[7] Aza Raskin, Privacy Icons: The Alpha Release, Aza Raskin's Personal Blog (July 7, 2015) http://www.azarask.in/blog/post/privacy-icons/.

[8] ESRB Privacy Certified Member Services, Entertainment Software Rating Board, http://www.esrb.org/privacy/member_services.jsp.

[9] Disconnect, https://disconnect.me/#about.

[10] TRUSTe Certification Standards, https://www.truste.com/privacy-certification-standards/.

[11] BBB Accreditation Standards, Better Business Bureau, http://www.bbb.org/council/for-businesses/about-bbb-accreditation/bbb-accreditation-standards/.

[12] Mary J. Culnan & Manoj Hastak, Future of Privacy Forum Online Behavioral Advertising "Icon" Study, Jan. 2010, *available at* http://www.futureofprivacy.org/2010/02/15/online-behavioral-advertising-icon-study/.

[13] Reidenberg, J. Breaux T, Cranor, L et al, Disagreeable Privacy Policies: Mismatches between meaning and users' understanding, Berkeley Technology Law Journal 30:1, pp. 39-88 (2015).

[14] Agreement Containing Consent Order, In the Matter of FTC True Ultimate Standards Everywhere, Inc., a corporation,) d/b/a TRUSTe, Inc., FTC File No. 1323219, (Nov. 17, 2014), https://www.ftc.gov/system/files/documents/cases/141117trusteagree.pdf.

[15] Reidenberg, J., Bhatia, J, Breaux, T. and T. Norton, Privacy Policy Ambiguity and the Impact of Regulation, J. Legal Studies, Vol. 45, *forthcoming*, http://ssrn.com/abstract=2715164.