Systematic Analysis and Evaluation of Web Privacy Policies and Implementations

Brad Miller
UC Berkeley
bmiller1@cs.berkeley.edu

Kaitlyn Buck
Microsoft
kaitlyn.buck@berkeley.edu

J.D. Tygar
UC Berkeley
tygar@cs.berkeley.edu

***Abstract*—In this research work, we introduce the first metric for systematic analysis and evaluation of a website's entire approach to online privacy. Since the user is the ultimate judge of whether privacy was acceptably maintained, our metric views all aspects of the privacy implementation from the perspective of usability. By examining the privacy policy, technical implementation and customizable features and interface from the perspective of usability, our metric identifies modifications to privacy policies and implementations which would improve user privacy outcomes *in practice*. Our work is motivated by the potential of improved privacy metrics to help organizations systematically identify and implement improvements in their privacy practices and interfaces. We evaluated ten websites using our metric and reveal potential for improvement in all websites as well as contrasts between websites with similar functions, such as social networking, online shopping and information retrieval.**

***Index Terms*—Privacy, Human factors, Usability testing, Measurement techniques**

I. Introduction

The ever increasing range and availability of web services with personalized or social aspects creates new security and privacy risks for users. Many problems result from users either not fully understanding the privacy practices of a website or failing to use the privacy features in a manner consistent with their goals. These usability deficits often have an impact on users comparable to or worse than back-end security breaches, as reflected in lawsuits and user complaints [14], [20].

There are several reasons that usability deficits persist despite the significant cost to both organizations and users. First, designing usable *privacy* interfaces presents a challenge distinct from designing usable interfaces *in general*, as evidenced by the large body of usable security research [21], [4]. Second, although users are offended by breaches of privacy, users seem to view privacy more as a baseline expectation than a feature on which to base product selection decisions. Even when users are explicitly told that one site is more private than another, users will pay only a small premium for the more private site [6], [23], likely believing that all sites will offer some basic level of privacy. Since improvements in privacy require specialized and expensive personnel and result in limited direct or immediate gain in user base, competitive pressure encourages organizations to invest resources elsewhere.

We introduce a metric that systematically identifies weaknesses in a website's approach to privacy. Such a metric may improve privacy outcomes by helping organizations to examine their own privacy practices and interfaces. Our metric focuses on the privacy which a user is likely to experience *in practice* while using a website. We refer to the privacy experienced in practice as the *effective user privacy* and view this term as representing the combined effectiveness of all privacy relevant aspects of a website, including privacy policy and underlying implementation, evaluated from the perspective of usability.

The objective of maximizing effective user privacy stands in contrast to the narrower approaches taken by privacy seals and privacy policy visualization tools. Privacy seals tend to focus on the completeness of the details specified in the privacy policy, place little emphasis on implementation details or cover them only in relation to personally identifiable information, and neglect usability entirely [2], [22]. In contrast, privacy policy visualization tools focus on presenting privacy information in a manner easily comprehensible to users [12], [13], [15], [19].

Unfortunately, the effectiveness of policy-centric approaches is limited by two assumptions. First, users must view the privacy policy. Second, having presumably understood the privacy policy and designed a compatible privacy goal, users must use the website in a manner consistent with their goal. To avoid the limitations inherent to these assumptions, our metric is divided into seven sections which comprehensively examine the website's privacy. The aspects examined by our metric include the completeness and content of the privacy policy, client storage and tracking practices, data handling practices and policies, and usability.

Although primarily designed as a resource for organizations offering services on websites, our metric can be evaluated by a skilled third party. We evaluated ten websites using our proposed metric. Our metric succeeded in identifying privacy strengths and weaknesses of each site, thereby implicitly identifying areas in which all sites could improve.

Throughout the remainder of this paper we present and evaluate the proposed metric. Section II discusses related work, including industry privacy seals and existing regulations in the EU and US. Section III discusses the design principles

Kaitlyn Buck participated in this work while attend UC Berkeley as an undergraduate. Kaitlyn graduated in December 2011 and was a full time employee of Microsoft at time of publication.

We gratefully acknowledge support from the National Science Foundation (through the TRUST STC) and the US State Department. The opinions in this paper are those of the authors and do not necessarily reflect those of funding sponsors.

used to develop our metric, and Section IV presents the metric itself. In Section V we evaluate the metric, and in Section VI we conclude.

II. Related Work

There are several topics in prior academic work, industry standards and governmental regulation related to our work. These areas are tangential to the metric which we propose, often having a narrower focus with less usability emphasis.

One area of related work examines the overall *readability* of privacy policies. Milne *et al.* and Jensen *et al.* apply standardized metrics, such as the Flesch Grade Level (FGL), to determine the readability of privacy policies [10], [16]. This technique reveals that privacy policies are often written at a college reading level, exceeding the education of many internet users. Proctor and Vu examine the readability of privacy policies in user studies, concluding that users are often unable to understand policies even if they do have the education indicated by the FGL [18], [25].

Similar to assessing the readability of privacy policies, a related area attempts to examine and identify improved ways of formatting privacy policies for presentation to users. The law firm Hunton & Williams developed a standardized format beginning with a short policy summary which has achieved limited industry adoption [9]. There has also been considerable work on expressing P3P policies to users, both graphically [12], [13], [19] and textually [13], [15]. This work relates to ours by seeking to identify areas of privacy concern for the user and to distinguish effective communications of privacy policies to users, but does not include aspects of usability or website implementation.

Separate from efforts focused on formatting and readability, there have also been efforts to improve the privacy policy authoring process. Karat *et al.* propose a tool designed to benefit users by generating policies which are more complete and benefit organizations by facilitating enforcement and abstract representation of the privacy policy [11].

Outside of privacy and general usability, related work has examined metrics for the accessibility of a website to people with disabilities. The W3C maintains the Web Content Accessibility Guidelines, a list of checkpoints which websites should satisfy in order to achieve different levels of accessibility [26].

Industry standards have also emerged that certify websites as maintaining minimum standards of privacy practices. The Better Business Bureau, Privacy Score and TRUSTe have developed certification programs and seal images which companies can display to indicate their privacy practices [2], [17], [22]. These certification programs tend to focus more on disclosure of privacy practices, deemphasizing technical or usability aspects of the implementation.

Our work also relates to governmental regulations in both the EU and US. Regulations in the EU tend towards a comprehensive approach, requiring minimum levels of privacy practice disclosure, data integrity, user access and user choice across all organizations but making no requirements about website design or usability. In contrast, privacy regulations in the US are tailored to specific sectors, such as COPPA (children's privacy), HIPAA (healthcare) and GLB (financial) [3], [7], [8]. Since privacy protections are generally stronger in the EU than the US, safe harbor programs have been established to allow US organizations to legally handle private data of EU residents. However, participation in these programs is far from universal, leaving ample opportunity for users both within and outside of the EU to interact with websites outside of the safe harbor [24].

III. metric Design Principles

Our approach to developing a metric to aid the design and implementation of privacy for a website focuses on the user's experience. Necessarily, this requires examining all aspects of privacy including privacy policy, implementation, and customizable settings from the perspective of usability. For example, we extend our evaluation to the types of tracking technologies used since some are easier for privacy conscious users to remove than others. Evaluation emphasizing usability results in a more complete understanding of the website from the user's perspective.

Although our primary objective is to aid organizations offering services over websites, we also chose to design a metric which a third party can use to review privacy practices without involvement from the organization itself. This allows independent organizations such as consumer advocacy groups to use the metric in comparing the privacy offered by competing websites. Since the complex and circumstantial nature of privacy prevents direct comparison of two sites based on their total metric scores, the metric is best used as an aid to guide the evaluation and identify potential points of difference.

The individual metric questions are also designed to have answers on an integer scale from 0 to 4, with 4 indicating the most private practice and 0 indicating the least private practice. Some metrics have a binary value, such as "Does the website use Flash Local Storage Objects (LSOs)?" In these cases lower values may be used to indicate more aggressive use of Flash LSOs, such as setting LSOs on pages which otherwise would not require the use of Flash. We hope that by restricting answers to a relatively narrow scope, we can avoid mandating particular design decisions and leave as much flexibility to the designer as possible while still distinguishing practices which will ultimately increase user privacy.

IV. Effective User Privacy metric

In this section we present our metric for improving effective user privacy. Recall that the effective user privacy is designed to be a representation of the total amount of privacy which is actually experienced by the user, and therefore must reflect the privacy practices, features and usability of the website. We have divided the metric into seven sections, each focusing on a different aspect of effective user privacy. The first five sections are designed to be applicable to any website, and the last two sections apply only to websites where the user has opened an account.

A. Privacy Document Accessibility and Readability

Although privacy policy requirements vary with jurisdiction and type of content, privacy policies have become commonplace and can be found on nearly all websites. In some cases, a website's privacy policy may be spread across several documents, possibly none of which may be titled the "Privacy Policy." For this reason the metric makes reference to *privacy documents*. Since the privacy documents are the most basic and ubiquitous tool for assessing the privacy practices of a website, users must be reasonably able to locate and understand the privacy documents.

1) Does the website offer a single, comprehensive document referred to as the "privacy policy" which describes the privacy practices of the website?
2) Does the website homepage use the word "privacy" in a link to either the privacy policy or a dedicated section of the website which contains any privacy documents?
3) Does the main privacy document begin with a summary of the entire policy and a section of links which help the reader to navigate the content?
4) Do the privacy documents include definitions that use laymans terms to explain privacy relevant aspects of any technical or legal terms?
5) Does the website offer a P3P formatted privacy policy?
6) Do the privacy documents indicate the last date they were updated?
7) Does the website offer to notify users of changes to the privacy documents?

The summary section recognized by metric 3 is the distinguishing feature of the standardized layered policy format developed by the law firm Hunton & Williams [9] and adopted by Microsoft, IBM, Proctor and Gamble, Hertz and Walmart, among others. The layered format increases both user speed and satisfaction while remaining as accurate as a traditional policy [13]. Metric 5 rewards sites which provide a P3P version of the privacy policy since Internet Explorer uses P3P as part of the default privacy settings [5].

B. Privacy Document Scope

Privacy documents can remain silent on important issues without attracting the attention of the user. This makes it harder for a user to gain a true understanding of the organization's privacy practices. As the scope of topics addressed in the documents contributes to effective user privacy, the metric rewards websites which offer comprehensive and forthcoming privacy documents. Note that metric questions in this section are concerned only with the disclosure of privacy practices and not with the practices themselves.

8) Do the privacy documents contain an unambiguous and clear explanation of the information collected by the website?
9) Do the privacy documents provide an exhaustive list of methods the website uses to collect information, such as HTTP cookies, web bugs and Flash Locally Stored Objects (LSOs)?
10) Do the privacy documents state how collected information will be used?
11) Do the privacy documents state which information will be shared with third parties, and for what purposes?
12) Do the privacy documents state any measures taken to protect data in transmission and in storage?
13) Do the privacy documents state how long data will be stored after collection by the website or deletion by the user?
14) Do the privacy documents contain an email address and a postal addresses for contacting the organization?

Note that metric 8 requires websites such as Google and Facebook which frequently supply content to third party sites to explain that user data gathered will extend beyond `google.com` and `facebook.com`, respectively. Organizations must also explain the extent and implications of log data gathered in terms understandable by the user.

C. Client Storage Practice and Policy

The ability of a website to associate multiple requests with a single user depends on associating a consistent, unique identifier with each request. Websites typically accomplish this using some form of storage on the client. Since some forms of client storage are more widely understood than others, the metric considers each potential form of storage separately in order to estimate the true usability barrier to removing any tracking data. The metric also considers steps which the website may take to support or penalize users who have disabled client storage mechanisms.

15) Does the website use HTTP cookies?
16) Does the website use HTML5 Local Storage or other non-cookie browser storage?
17) Does the website use Flash LSOs?
18) Does the website become significantly less useful if HTTP cookies or other browser storage is disabled?
19) If the website uses Flash LSOs, does the website become significantly less useful if Flash is disabled?
20) If the website uses cookies, do the privacy documents accurately describe the use of HTTP cookies?
21) If the website uses Flash LSOs or browser storage other than cookies, do the privacy documents accurately describe these practices?
22) Do the privacy documents accurately explain the extent to which the user can avoid client storage based tracking and guide the user through that process?

Note that in evaluating metrics 18 and 19, portions of the website which are accessible only after log-in should be disregarded.

D. Third Party Tracking Practice and Policy

Third party tracking presents a significant threat to privacy usability since users are unable to directly observe any evidence of the tracking, making the understanding that a third party is observing communication counterintuitive. The following metrics examine third party tracking from the perspectives of both employing and offering third party trackers.

23) Does the website use any resources hosted by third parties, such as web beacons or Javascript libraries?
24) Does the website generate any requests to third parties which include a persistent cookie?
25) Does the website continue to function if browser extensions blocking third party tracking are used?
26) Does the website make any requests to third parties which are not blocked by browser extensions blocking third party tracking, such as Javascript libraries?
27) Does the organization associated with the website offer any web plug-ins designed to be used on third party sites?
28) Do the privacy documents guarantee the user the right to opt-out of non-critical information sharing with third parties and explain any technical measures necessary to do so, such as opt-out cookies?

Metric 23 distinguishes the use of web beacons since these can only be prevented by a browser extension. Metric 26 is designed to detect the integration of third party content which the user is effectively unable to remove, such as script libraries that leak information to third parties by the act of loading the library. Metric 27 identifies organizations which offer web plug-ins, such as "like" buttons and ads, that can be integrated by other websites and allow gathering information across domains.

E. Data Handling Practice and Policy

The following metrics address ways in which organizations use and protect user data, as well as ways that organizations allow a user access to data pertaining to herself. Sound data handling practices have the potential to increase the usable privacy of the website by providing security and privacy by default. Data access measures help users to understand the scope of data collection.

29) Does the privacy policy allow targeting either advertising or content to the user?
30) Does the entire website support HTTPS?
31) Does the entire website use HTTPS by default?
32) Does the website provide features for accessing the data which is stored about the user?
33) Does the website provide features for modifying or deleting data which is stored about the user?
34) Do the privacy documents guarantee the user rights to access, modify or delete data about the user and provide guidance to do so?
35) Do the privacy documents allow data collected from or deleted by the user to be retained longer than is legally necessary?

Metrics 32, 33 and 34 reward allowing the user to access, review and modify information associated with the user. While this may seem more appropriate for websites at which the user has opened an account, given the breadth of data which third party tracking organizations can obtain about users, data access mechanism seem appropriate in situations where the user may not have an account.

F. Personal Account Information

The following metrics are designed to be applied only to websites which support user accounts and deal with the handling of information associated with accounts. As the range of information-sharing features and goals varies from one website to the next, these metrics are most useful for comparing the privacy of websites which serve a similar purpose from the user's perspective.

36) Does the website request the user's phone number for an activity where the user's primary goal is not to receive a phone call or use two factor authentication?
37) Does the website request the user's physical address for an activity where the user's primary goal is not to receive physical mail?
38) Do the privacy documents allow any contact information to be used for marketing purposes?
39) Do the privacy documents allow third parties to use any contact information for marketing purposes?
40) Do the privacy documents allow the user to opt out of non-critical mailings?
41) Do the privacy documents state what user information will be publicly visible, either by default or at minimum?
42) If the organization offers plug-ins for use by third party websites, do the privacy documents guarantee that any data obtained from plug-ins will not be linked to data entered at the organization's website?
43) If the website facilitates sharing data with other users and the public, does the website provide mechanisms for defining access policies at the granularity of individual users as opposed to differentiating between groups of users or using the same policy for all users?
44) If the website facilitates sharing data with other users and the public, does the website allow different access policies to be associated with different types of data, or preferably with different instances of the same type of data?

G. Privacy Customization Usability

This section examines the usability of privacy settings accessible to users who have opened an account on a website. As with the previous section, the range of privacy settings will vary with the context of the website, so these metrics are most useful for comparing websites that serve a similar purpose to the user. The metrics are also universal enough to serve as a usable design aid for a range of privacy user interfaces.

45) Does the account setup process include selecting privacy settings?
46) Do all privacy settings default to the most private setting available?
47) Does the website have a section dedicated to privacy settings and containing all privacy settings applicable to the whole website?
48) Does either the website homepage, a menu on the site homepage, or the account settings page contain a link to the privacy settings page?

TABLE I: Evaluation of sites on which the user has opened an account.

Metric Area	Max Score	Google	Facebook	Twitter	Amazon	Ebay	Overstock
Privacy Document Accessibility	28	19	17	17	18	22	15
Privacy Document Scope	28	23	16	22	18	23	26
Browser Storage	32	15	18	18	16	20	19
Third Party Tracking	24	17	18	13	13	12	12
Data Handling	28	16	16	15	13	7	9
Personal Account Information	36	26	21	20	17	16	25
Privacy Customization Usability	36	23	19	25	18	19	23
Total (raw)	212	139	125	130	113	119	129
Total (scaled)	100.0	65.6	59.0	61.3	53.3	56.1	60.8

TABLE II: Evaluation of sites on which the user strictly consumes content.

Metric Area	Max Score	Wikipedia	Library of Congress	Alcoholics Anonymous	New York Times
Privacy Document Accessibility	28	15	17	17	19
Privacy Document Scope	28	22	20	19	19
Browser Storage	32	26	16	26	16
Third Party Tracking	24	24	16	16	12
Data Handling	28	7	4	4	2
Total (raw)	140	94	73	82	68
Total (scaled)	100.0	67.1	52.1	58.6	48.6

49) Does the website describe each privacy option in detail?
50) Are descriptions of what each privacy setting entails directly accessible from where the user would alter the privacy settings?
51) Does the website provide active tips or guidance the first time each privacy setting or privacy sensitive feature is used or adjusted?
52) Does changing an aspect of the privacy settings ever require more knowledge of computer security than a lay person has?
53) Does the website provide any information about computer security necessary to help the user select privacy settings?

V. Evaluation

This section presents an application of the metric to ten websites. Table I presents our examination of websites at which we assume the user has opened an account, including three online social networks and three shopping related websites. Table II presents our examination of four websites at which we assume the user does not open an account or enter any personal information and seeks only to retrieve information. Recall that the Personal Account Information and Privacy Customization sections of the metric apply only to websites on which the user opens an account. Raw scores from our evaluation can be seen in the Appendix.

We conducted our evaluation on a virtual machine running Ubuntu using the Chrome browser with the Ghostery and Do Not Track Plus extensions for blocking third party tracking, and the Privacy Bird extension for determining P3P compliance. We also checked request headers for compact P3P policies not detected by the Privacy Bird extension. We manually examined request logs to check for the presence of third party content not detected by the Ghostery and Do Not Track Plus extensions, such as Javascript libraries. In order to determine the client storage techniques used by the website, we cleared all client storage, browsed several sections of the website, opened an account if appropriate and then logged in and continued browsing, and rechecked client storage for the presence of tracking devices. The evaluation was conducted during May 2012.

In interpreting the results, notice that nearly *all* websites have significant room for improvement in *all* categories, indicating that the metric can identify weaknesses in privacy implementations across a range of websites. Furthermore, the full results show that of the full set of 53 metrics, there were only four metrics for which the maximum score was 3, and five metrics for which the maximum score was 2, the remaining metrics having received at least one score of 4. This implies that a website which combined the best aspects of all websites would receive a scaled score of 93.4. This significantly exceeds the maximum of 67.1 observed in the actual scores and illustrates the metric's ability to identify improvements in a broad range of websites.

Also, notice that the performance of websites with respect to a particular metric section generally correlates to the website category, reflecting variations in the privacy risk posed by different types of websites. That said, there remain distinctions in the performance of websites in the same category, providing guidance for users in selecting a service provider.

Examining the results more closely, the contrast in performance between Google and Facebook illustrates the metric's ability to identify reasonable improvements to privacy policies and implementations. Notice that Google has received a higher score for Privacy Document Scope and Facebook received a higher score for Browser Storage. This is because Google's "privacy policy" reasonably described Google's use of tracking techniques as well as data use, where as Facebook's "data use policy" overlooked tracking techniques and focused more exclusively on data use. Interestingly, Google's actual use of client storage was more invasive than Facebook's, as Google used Flash LSOs more aggressively than Facebook. The metric successfully rewards both Google for disclosure and Facebook for private practices, while identifying easy and concrete ways for Facebook to improve user understanding of privacy features.

The Library of Congress and Wikipedia also present an interesting privacy contrast. Although libraries are normally vigilant of patron privacy, we see that the Library of Congress receives the second lowest privacy rating of all the sites surveyed and Wikipedia receives the highest. This discrepancy stems largely from the use of client storage and third party tracking, technical areas in which Wikipedia dominates by avoiding the use of Local Storage, Flash LSOs and persistent cookies that identify the user. Since Local Storage and Flash LSOs have uses outside of client tracking, the Library of Congress may be using these features as part of software packages or libraries without realizing the privacy implications. By applying a metric designed to aid non-privacy experts in privacy evaluation, the Library could potentially discover and change these practices.

In a similar error, our evaluation of the Alcoholics Anonymous website revealed requests to `yui.yahooapis.com` (owned by Yahoo!) for script libraries. These requests included a referrer header showing the `aa.org` domain as well as a cookie, having the effect of telling Yahoo that the user was visiting Alcoholics Anonymous. Since the Alcoholics Anonymous privacy policy guarantees "strict confidentiality", this behavior may not be fully intended or understood by those responsible for the website [1].

VI. Conclusion

In this research work we introduced the first metric for evaluation of a website's entire approach to online privacy, including policy, implementation and usability. Our metric benefits organizations responsible for maintaining web services as well as consumer advocacy groups by providing a systematic method for reviewing privacy practices. We apply the 53 question metric to ten websites, and identify problematic behaviors and potential improvements in each site.

References

[1] Alcolholics Anonymous. http://aa.org, Accessed May 2012.

[2] Better Business Bureau. BBB accredited business seal for the web. http://www.bbb.org/us/bbb-online-business/, Accessed May 2012.

[3] Children's Online Privacy Protection Act. http://www.ftc.gov/ogc/coppa1.htm, Accessed May 2012.

[4] L. F. Cranor and S. Garfinkel. *Security and Usability: Designing Secure Systems That People Can Use*. O'Reilly Media, 2005.

[5] Dean Hachamovitch. Google bypassing user privacy settings. http://blogs.msdn.com/b/ie/archive/2012/02/20/google-bypassing-user-privacy-settings.aspx, Accessed May 2012.

[6] S. Egelman, J. Tsai, L. F. Cranor, and A. Acquisti. Timing is everything?: the effects of timing and placement of online privacy indicators. In *Proceedings of the 27th international conference on Human factors in computing systems*, CHI '09, 2009.

[7] Gramm-Leach-Bliley act. http://www.ftc.gov/privacy/glbact/glbsub1.htm, Accessed May 2012.

[8] Health information privacy. http://www.hhs.gov/ocr/privacy/, Accessed May 2012.

[9] Hunton & Williams. Ten steps to develop a multilayered privacy notice. http://www.informationpolicycentre.com/files/Uploads/Documents/Centre/Ten_Steps_whitepaper.pdf, Accessed May 2012.

[10] C. Jensen and C. Potts. 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, 2004.

[11] C.-M. Karat, J. Karat, C. Brodie, and J. Feng. Evaluating interfaces for privacy policy rule authoring. In *Proceedings of the SIGCHI conference on Human Factors in computing systems*, CHI '06, 2006.

[12] P. G. Kelley, J. Bresee, L. F. Cranor, and R. W. Reeder. A "nutrition label" for privacy. In *Proceedings of the 5th Symposium on Usable Privacy and Security*, SOUPS '09, 2009.

[13] P. G. Kelley, L. Cesca, J. Bresee, and L. F. Cranor. Standardizing privacy notices: an online study of the nutrition label approach. In *Proceedings of the 28th international conference on Human factors in computing systems*, CHI '10, pages 1573–1582, New York, NY, USA, 2010. ACM.

[14] J. LeClaire. Facebook Hit with $15 Billion Privacy Class Action Suit. http://business.newsfactor.com/story.xhtml?story_id=102009F7FD4C, Accessed June 2012.

[15] A. M. Mcdonald, R. W. Reeder, P. G. Kelley, and L. F. Cranor. A comparative study of online privacy policies and formats. In *Proceedings of the 9th International Symposium on Privacy Enhancing Technologies*, PETS '09, pages 37–55, Berlin, Heidelberg, 2009. Springer-Verlag.

[16] G. R. Milne, M. J. Culnan, and H. Greene. A longitudinal assessment of online privacy notice readability. *Journal of Public Policy & Marketing*, 25:238–249, 2006.

[17] Privacy Score. http://privacyscore.com/, Accessed May 2012.

[18] R. W. Proctor, M. A. Ali, and K.-P. L. Vu. Examining usability of web privacy policies. *Int. J. Hum. Comput. Interaction*, pages 307–328, 2008.

[19] R. W. Reeder, P. G. Kelley, A. M. McDonald, and L. F. Cranor. A user study of the expandable grid applied to p3p privacy policy visualization. In *Proceedings of the 7th ACM workshop on Privacy in the electronic society*, WPES '08, pages 45–54, New York, NY, USA, 2008. ACM.

[20] C. Scott. User Vote on Facebook Privacy Policies Hasn't Stemmed Criticism. http://www.pcworld.com/businesscenter/article/257101/user_vote_on_facebook_privacy_policies_hasnt_stemmed_criticism.html, Accessed June 2012.

[21] Symposium on usable privacy and security. http://cups.cs.cmu.edu/soups/2012/, Accessed October 2012.

[22] TRUSTe Website Privacy Solutions. http://www.truste.com/products-and-services/enterprise_privacy/web_privacy_seal, Accessed May 2012.

[23] J. Y. Tsai, S. Egelman, L. Cranor, and A. Acquisti. The effect of online privacy information on purchasing behavior: An experimental study. *Info. Sys. Research*, 22(2), June 2011.

[24] US-EU Safe Harbor Framework. http://export.gov/safeharbor/, Accessed May 2012.

[25] K.-P. L. Vu, V. Chambers, F. P. Garcia, B. Creekmur, J. Sulaitis, D. Nelson, R. Pierce, and R. W. Proctor. How users read and comprehend privacy policies. In *Proceedings of the 2007 conference on Human interface: Part II*, 2007.

[26] W3C web content accessibility guidelines. http://www.w3.org/TR/WCAG20/, Accessed May 2012.

Appendix

The Appendix presents the raw scores from the metric evaluation. Note that metric sections F and G do not apply to Wikipedia, The Library of Congress, Alcoholics Anonymous or the New York Times.

TABLE III: Raw scores from metric evaluation.

	Index	*Google*	*Facebook*	*Twitter*	*Wikipedia*	*Library of Congress*	*Alcoholics Anonymous*	*New York Times*	*Amazon*	*Ebay*	*Overstock*
Document Accessibility	1	4	3	4	4	4	4	4	3	3	4
	2	4	4	4	3	2	4	4	4	4	4
	3	0	2	0	2	4	2	2	2	3	0
	4	4	2	2	2	3	3	2	2	2	1
	5	0	0	0	0	0	0	0	2	4	2
	6	4	4	4	4	4	4	4	4	4	4
	7	3	2	3	0	0	0	3	1	2	0
Document Scope	8	3	3	4	3	4	3	3	4	4	3
	9	2	1	4	4	2	4	2	3	3	4
	10	4	3	4	4	4	4	4	3	4	4
	11	4	2	4	4	4	4	4	4	4	4
	12	4	0	0	2	2	1	4	2	2	4
	13	4	3	4	2	2	0	0	0	2	3
	14	2	4	2	3	2	3	2	2	4	4
Browser Storage	15	0	0	0	2	0	0	0	0	0	0
	16	0	0	0	4	0	4	0	0	4	0
	17	0	3	4	4	0	4	4	0	0	4
	18	4	4	4	4	4	4	0	3	3	3
	19	3	4	4	4	3	4	4	4	4	4
	20	4	4	4	3	4	4	4	4	4	4
	21	2	2	0	4	1	4	2	2	3	2
	22	2	1	2	1	4	2	2	3	2	2
Third Party Tracking	23	4	4	0	4	0	0	0	0	0	0
	24	4	4	2	4	2	4	0	0	0	0
	25	4	4	4	4	4	4	4	4	4	4
	26	4	4	4	4	4	0	0	4	0	0
	27	0	0	0	4	4	4	4	1	4	4
	28	1	2	3	4	2	4	4	4	4	4
Data Handling	29	0	0	0	3	4	4	0	0	0	0
	30	3	3	3	4	0	0	2	2	1	2
	31	2	2	3	0	0	0	0	2	1	2
	32	4	3	2	0	0	0	0	3	2	1
	33	4	3	2	0	0	0	0	3	2	1
	34	3	2	1	0	0	0	0	3	1	1
	35	0	3	4	0	0	0	0	0	0	2
Personal Information	36	3	3	3	-	-	-	-	3	0	3
	37	3	3	4	-	-	-	-	4	0	4
	38	2	2	0	-	-	-	-	1	0	2
	39	4	2	4	-	-	-	-	2	2	4
	40	2	1	4	-	-	-	-	4	4	4
	41	2	3	3	-	-	-	-	0	4	2
	42	2	0	1	-	-	-	-	1	4	4
	43	4	4	1	-	-	-	-	1	1	1
	44	4	3	0	-	-	-	-	1	1	1
Privacy Customization Usability	45	1	0	0	-	-	-	-	0	0	2
	46	1	1	2	-	-	-	-	1	0	0
	47	2	3	4	-	-	-	-	3	3	3
	48	4	4	3	-	-	-	-	3	3	4
	49	4	4	4	-	-	-	-	3	3	3
	50	2	3	4	-	-	-	-	1	4	3
	51	1	1	0	-	-	-	-	1	0	2
	52	4	2	4	-	-	-	-	3	3	3
	53	4	1	4	-	-	-	-	3	3	3