Are They Worth Reading? An In-depth Analysis of Online Advertising Companies’ Privacy Policies

Lorrie Faith Cranor,1 Candice Hoke,1 Pedro Giovanni Leon,1 and Alyssa Au2

1Carnegie Mellon University
2University of Pittsburgh

Privacy policies are often notoriously difficult for consumers to read and understand due to the use of legalistic and sometimes ambiguous language. This project analyzed the privacy policies published by companies that specialize in online tracking of consumers’ Internet activity. We analyzed 53 distinct practices pertaining to collection, aggregation, sale and management of consumer data, including sharing, retention and deletion of data, security measures for data management, among others. Known as the Online Behavioral Advertising (OBA) industry, these companies track Internet users’ online activities across sites and webpages ostensibly to deliver ads that are more likely to be relevant to them. While the advertising industry has attempted to self-regulate, Internet users, policy makers, and privacy scholars have raised concerns about the lack of transparency and user control.

In the current self-regulatory regime, OBA companies are directed to publish privacy policies to provide consumer notice and offer opt-out choices.1 However, it remains unclear whether the information these policies provide would allow users to understand companies’ practices and take actions to control the collection and use of their information. Therefore, we attempt to answer the following questions:

(1) What is the proportion of OBA companies participating in industry self-governance versus those not?

(2) Are there consumer-relevant differences in the privacy policy terms as between the firms affiliated with industry self-governance and those who are not? For instance, do the OBA-affiliated firms publish policies that accord with the FTC’s consumer protection requirements at a greater rate and with greater completeness than those not affiliated with industry self-governance?

(3) Are certain policies relevant to consumers, such as retention period and sharing with third-parties that will merge received data with other data streams, clearly stated in language average consumers can understand, or are the policies vague or silent on these and other practices?

(4) Do the policies clearly state consumers’ choices about OBA tracking that collects their data and offer conspicuous mechanisms to implement those choices?

To answer these questions, in January of 2014 we retrieved a comprehensive list of tracking companies from Evidon’s online database.2 Evidon listed 2,750 companies under various non-mutually exclusive categories including, ad networks, ad servers, ad exchanges, analytics, optimizers, supply and demand side platforms, data management platforms, and web publishers, among others. It also included the affiliations (if any) that these companies maintained with self-regulatory organizations. A large fraction (70%) of listed companies did not state any affiliations. From the remaining 815 (30%) companies, 540 stated affiliations with the primary industry self-

---

2 http://www.evidon.com/consumers-privacy/company-database
governance entities (either the Digital Advertising Alliance (DAA), the Interactive Advertising Bureau (IAB), or the Network Advertising Initiative (NAI)). The remaining 275 companies were affiliated only with weaker self-regulatory organizations. We also obtained a list of the 36 largest tracking companies, relying on the 2013 Evidon global report.\(^3\)

We first classified OBA companies into one of three categories: (1) “Large” companies, a sample of 28 randomly selected from the 36 largest tracking companies; 2) “Affiliated” companies, which are 23 companies that comprise a sample randomly selected from the set of companies listing affiliations with DAA, IAB, or NAI, and 3) “Unaffiliated” companies, which are 30 companies that comprise a sample randomly selected from the set of companies with no affiliations listed. These 81 firms’ privacy policies provided our analytic focus.

We expected to analyze privacy policies from the 81 online tracking companies randomly selected from Evidon’s public database. From the 81 companies, only 71 had a privacy policy, and from those, only 62 had a privacy policy intended for tracked users. “Large” companies and “affiliated” companies were more likely to have a privacy policy intended for tracked users. We found important differences among the evaluated policies, both with respect to disclosed practices and clarity. Our analysis allowed us to identify a number of areas that need improvement to better provide transparency about advertising companies’ practices.

Using the Evidon resources, we found that only 30% of online tracking companies were affiliated with self-regulatory organizations. Further, many companies seem to join such an organization only temporarily or fail to communicate that they are members in their privacy policies, as our set of 23 “Affiliated” companies (retrieved in January 2014) contained 12 companies that did not list any affiliations in their privacy policies. We do not know whether these companies are actually affiliated or not. One company that (according to Evidon) was not affiliated in January 2014, but listed affiliations in its privacy policy later, at the time we analyzed it. More than a third of companies in the “Large” set did not list any self-regulatory affiliations. Companies affiliated with self-governance failed to report practices that are required by self-regulatory principles including, retention period, collection of sensitive data types, and merging of PII with non-PII.

These results suggest that too few incentives and penalties currently exist to provide the inducements for OBA companies to join self-regulatory programs. The low rates of participation as affiliated companies, and the low rates of affiliated companies’ compliance with their own self-governance principles lead to serious questions regarding the adequacy of the current self-regulatory approach in protecting Internet users’ privacy. The uncontrolled and unspecified OBA information sharing practices may allow users’ information to propagate with unlimited restrictions.

From the privacy policy analysis, we were able to identify a large number of factors that reduce the capacity for user/consumer understanding and meaningful choices about OBA tracking and use of their data. For instance,

* Silence on the company’s data practices, including:
  * Opportunity to limit data collection or sharing,
  * Merging of PII with not-PII, retention period, and
  * Access opportunities for users to review and edit collected data about them
* Lack of standard definitions of terms to refer to third-parties, uses and data types;
* Lack of effective tools for indicating user choices, for instance, a link for users to opt out

\(^{3}\) http://www.evidon.com/research
• Mixing within one policy the data practices that apply to the company's data sharing partners and those that apply to tracked Internet users (rendering it very difficult to disentangle the practices that apply only to tracked users);

• Mixing within one policy the data practices that apply to it as a “first-party” website as well as well as its “third-party” (i.e., not user-facing) online tracking activities across other sites. Such companies include Google AdSense, Adobe, Yahoo, Apple, Verizon, and CBS. This policy mixture creates additional transparency and user control challenges.

Among our recommendations for moving forward, we believe that standardization of terminology is important to ease of user understanding. Such as step would facilitate standardization of privacy policies and empowerment of user/consumers, who could use automated tools to verify privacy policies. Automated tools would also facilitate supervisory entities' capacity to verify compliance. We additionally submit that some practices are more urgent to consumers’ privacy and safety online than others (for instance, choices to permit OBA tracking and sale/merger of PII with non-PII). The high priority privacy practices should be made salient in privacy policies, perhaps by using layered notices, instead of permitting them to be buried in long-winded, confusing policies. Finally, because our sample revealed some companies' policies written in foreign languages (understandable given the lack of geographical boundaries on the Internet), the task of harmonizing international privacy protection frameworks must be completed.