ROBERT GELLMAN
Privacy and Information Policy Consultant
419 Fifth Street SE
Washington, DC 20003

202-543-7923
bob@bobgellman.com
www.bobgellman.com

Lacking in Facts, Independence, and Credibility: The 2011 NAI Annual Compliance Report

Robert Gellman

July 2012
Version 1.2

Introduction and Summary

What is the value of privacy self-regulation? The source of rules for privacy and the degree of compliance with those rules remain significant issues in the United States and elsewhere around the world. The purpose of this short review is to contribute to ongoing evaluations of privacy self-regulation by examining a compliance report by the Network Advertising Initiative (NAI), a privacy self-regulatory organization with a somewhat checkered past.

The report in question is the Network Advertising Initiative's (NAI) 2011 Annual Compliance Report, http://www.networkadvertising.org/pdfs/NAI_2011_Compliance_Report.pdf.

Does the NAI's 2011 compliance report offer evidence that self-regulation is effective and worthwhile? The conclusions here are that the NAI report does not offer meaningful evidence that self-regulation is effective, that the report hides more than it reveals about the NAI compliance process, and that the value of non-independent self-regulatory audits is unproven. This analysis does not review the adequacy of the NAI Code.

Earlier reports raised serious questions about the bona fides of privacy self-regulation. In 2007, the World Privacy Forum (WPF) issued a report by Pam Dixon on the NAI's initial efforts at self-regulation for privacy. The report, *The NAI: Failing at Consumer Protection and at Self-Regulation*, http://www.worldprivacyforum.org/pdf/WPF_NAI_report_Nov2_2007fs.pdf, found that the efforts of the NAI failed to protect consumers and failed to self-regulate the behavioral targeting industry.

A 2011 WPF report by Robert Gellman and Pam Dixon took a broader look at self-regulation. *Many Failures: A Brief History of Privacy Self-Regulation in the United States*, http://www.worldprivacyforum.org/pdf/WPFselfregulationhistory.pdf. The report's central finding was that a majority of the industry privacy self-regulatory programs failed in one or more substantive ways, and that many of the programs disappeared when political pressure evaporated.

This analysis takes a different tack. It looks closely at a compliance report by the NAI to determine what the report shows about the value of the NAI's privacy self-regulation.

The NAI report provides carefully selected and edited information about its members, the audit process, the qualification of its auditors, and the independence of its auditors. The NAI report fails to provide enough context for the few facts that it does provide, uses weasel-worded statements that obscure the degree of compliance or non-compliance by NAI members, and claims credit for compliance with laws that are independent of NAI standards.

Any audit of privacy standards applicable to multiple organizations inevitably will find some examples of non-compliance with those standards. Perfection is not expected by anyone. A fair measure of self-regulation is regular reporting, independently conducted audits, and credibly reported results. Applying this standard, the NAI satisfies only the first element. It is difficult for a careful reader of the 2011 NAI report to determine how the NAI conducted its audits, to understand what facts the audit produced (as distinguished from broad and unsupported generalizations), or to give much credibility to the report's broad and overstated conclusions.

Lacking in Facts, Independence, and Credibility: The 2011 NAI Annual Compliance Report

Issue 1: Are all NAI members audited for compliance?

From the Report:

"NAI members become eligible for annual reviews in 'the year following admission to the NAI as a new member.'" Report at footnote 8.

"The Code requires all companies that have been NAI members for at least one year to undergo an annual review to help assess compliance with the Code." Executive Summary at page 1.

"For the 2011 annual compliance review, NAI staff reviewed the 60 companies that were NAI members as of January 1, 2010…" Report at page 6.

Comment: NAI requires no compliance audit for NAI members when they join or for as long as 11 plus months after they join. The report offers no explanation for the gap between joining the NAI and the required audit. Appendix A to the report lists 25 companies that joined in 2011 but were not subject to compliance audits. A member who joined on January 2, 2010 was not included in the 2011 compliance audit. Indeed, if a compliance audit were conducted in late in the following year, a member could go as long as 23 months without facing a compliance audit. If that member were audited, found wanting, and resigned before the report was completed, the report apparently would not show the failure to comply at all.

The report does not include the dates when members joined. The report does not identify whether any members resigned or when they resigned. The report does not state when audits started or ended. The lack of full disclosure makes it difficult to tell if NAI manipulated compliance reporting to avoid revealing a lack of compliance or a lack of auditing.

Issue 2: Lack of denominators

From the Report:

"There were nearly 8.5 million unique visits to the NAI's website, reflecting a nearly 200% increase over 2010. In addition, there were nearly six million unique visits to the NAI's opt-out page, a 162% increase over the prior year. Of those visitors, 840,000 unique users submitted requests to opt out of OBA by one or more NAI member company. The website's educational section also showed enormous growth, with more than 2.5 million unique page views last year. This increased attention is due in large part to NAI members, who continued their efforts to educate consumers about OBA by contributing more than 4.1 billion ad impressions to the NAI's OBA awareness campaign in 2011." Executive Summary at page 1.

Comment: The reported numbers are large and seem impressive, but many Internet usage statistics include large numbers. Raw numbers mean little. The NAI report fails to include any denominators that might give meaning to the reported numbers. The proper issue is whether the NAI opt-out was effective. If 4.1 billion ad impressions resulted in 840,000 opt-outs, that is a conversion rate of just over .02%. To put this number in perspective, the conversion rate would have to increase by nearly a factor of 50 to reach one percent.

Can a program be successful by any standard if it results in attracting a tiny fraction of one percent of users? It seems likely that concern about privacy among the general Internet population is greater than that. Opt-out programs rarely work well under most circumstances (which is why industry provides opt-outs) and tend to attract only a few percent of users. Two one-hundredths of 1 percent does not even meet the already lowered expectations for a privacy opt-out.

Other facts are missing. Were the ad impressions seen by U.S. consumers or by consumers in other countries? The report does not state whether opt-outs came from consumers in the U.S. or elsewhere. Is the proper denominator the number of U.S. Internet users or the number of international Internet users? The NAI does not tell us what it thinks a proper denominator should be. Perhaps the NAI does not want to establish a standard that might be used to judge its activities.

It is difficult to make much of these numbers. If any commercial ad program had such a low conversion rate, it would be proclaimed a failure and pulled immediately.

Issue 3: Weasel-worded statements

The Report's Executive Summary was carefully written to give the impression that NAI members met the required standards without revealing the extent to which compliance was lacking.

> From the Report:
>
> The 2011 NAI Annual Compliance Report "demonstrated that, ***on the whole***, evaluated member companies ***fully met*** their compliance obligations. The review also identified several areas in which the NAI and its members could improve." Executive Summary at page 1 (emphasis added).

Comment: What does *on the whole* mean? What does it mean to say that companies *fully met* their obligation modified in this way. *On the whole* means something less than *fully*. *On the whole* means for the most part or apart from some insignificant details. The language in the two quoted sentences seems to be an intentional welter of confusion. If companies *fully met* obligations, then there would be no need for a modifier suggesting that compliance was not entirely complete. Further, if there were full compliance, then why did the report identify areas where members could improve? If a company fully complied, then there would be no room for improvement. This language calls into question the credibility of the entire report. There would be nothing wrong with reporting a modest amount of non-compliance with standards. Perfection

is not a requirement for an effective compliance program. However, reporting full compliance is not credible. Artfully written claims only suggest that more is being hidden than is being revealed.

From the Report:

"NAI staff uncovered ***brief and isolated*** issues with specific opt-out mechanisms." Report at page 2 (emphasis added).

Comment: The reader has no idea what either *brief* or *isolated* means. These vague words could mean anything at all. The report offers no numbers and no metrics. The statement conveys no real information, and the lack of data suggests that the report may be hiding something.

From the Report:

"The review revealed very few ***potential*** compliance deficiencies." Report at page 3 (emphasis added).

Comment: The highlighted word is noteworthy. What is a *potential* compliance deficiency? It is hard to believe that any set of rules does not raise the possibility of numerous *potential* compliance deficiencies. There are usually many theoretical ways *not* to comply with a rule. It appears that the quoted statement essentially says nothing. The report deliberately chose to use a meaningless phrase rather than offer substantive information or discuss *actual* compliance deficiencies. A better compliance report would provide firm numbers and details rather than vague phrases like *very few*. It is not credible that there were no actual compliance deficiencies among all the members of the NAI.

From the Report:

"Standard

When member companies provide non-aggregate non-PII to third parties to be merged with PII possessed by the third parties for OBA or Multi-Site Advertising services, they must contractually require the third parties to adhere to applicable provisions of the Code. (NAI Code § III.5(b).)

Findings

This provision of the Code governs data that is not PII, and is not aggregated before being shared with another party, and thus is user-level non-PII. No evaluated members were found to share user-level non-PII ***with the intent of it being merged with PII***. Most member companies do not share user-level data with anyone other than service providers. Those companies that do share user-level data with third parties ***generally*** contractually forbid receiving parties from merging the data with PII. NAI staff's review of those contractual provisions and

> members' internal policies with respect to the sharing of user-level non-PII demonstrate that members seek to ensure that such data is not merged with PII and is protected in accordance with the NAI Code." Report at page 23 (emphasis added).

Comment: Why does the Report state that non-PII was not shared with the *intent of it being merged with PII*? Was it shared and merged *without* intent? The reliance on the qualifier *with the intent* raises another question about the credibility of the report. The statement is not the same thing as a flat denial that non-PII was shared and merged with PII.

Further, it is not at all clear what the word *generally* means. If contractual requirements are an obligation, then either all companies either do or do not comply. The word *generally* suggests that some or most companies meet the requirement. However, all that the reader receives is a vague suggestion that implies compliance without a precise set of findings. The use of weasel words here makes it difficult to assess the report's conclusion, other than to question its credibility and transparency.

Issue 4: No Independent Audit

> From the Report:
>
> "For the 2011 annual compliance review, NAI staff reviewed the 60 companies that were NAI members as of January 1, 2010…" Report at page 6.

Financial audits of public companies are conducted by independent accounting firms. Few would accept the results of an audit conducted by auditors that have an interest in the results. Yet it appears that NAI compliance audits are conducted by NAI staff, who cannot be characterized as anything other than interested parties. If an NAI audit uncovers too many problems, the NAI faces the possibility of losing members, and the auditors could lose their employment. Nothing is more fundamental to an audit than independence, objectivity, and impartiality. All three appear lacking in the NAI audit process.

The NAI compliance report does not include any information on the qualifications or experience of the NAI staff. It is unknown if they perform other functions for NAI or if they have relationships with member companies that extend beyond the audit. It is unknown if any aspect of their employment is determined in any way by the results of their audits or their relationships with member companies.

The absence of any findings about individual companies leaves the compliance report with virtually no detailed information other than a general description of the process together with broad and vague conclusions about compliance by NAI members as a group. There is no discussion about individual companies or specific evidence about the details of the compliance review for those companies. The report includes no factual support for the report's conclusions. The reader has only the self-serving conclusion from non-independent auditors that NAI members are in compliance but without documentary support or supporting evidence.

It may be telling that the report's only instance (Report at 19) of non-compliance by a named NAI member company came to light because of work done by and made public by the Stanford's Center for Internet and Society. The report does not include a single instance of non-compliance by a member company identified by the NAI staff.

For example, in discussing opt-out cookies, the report states that "NAI staff has observed an increase in the reliability of members' opt-out cookies." Report at 18. This statement is wholly unexplained, does not identify any members, and includes no metrics or definition of *reliability*. The statement is not even qualified, offering no adjective to modify *increase*. Was the increase significant? Material? Was the increase from 1% to 1.1%? The increase may or may not have significance, but the reader cannot judge. The absence of a metric suggests that it would not have been favorable to the NAI to include one.

The report offers no information on individual companies or on which websites, domains, or functions were reviewed. Did the compliance review include sampling? There is no discussion about the thoroughness of the review. The report did not include a list of questions that auditors asked. There is nothing but a vague and unsupported conclusion about the membership as a whole by a non-independent audit staff.

It appears that the same NAI staff that conducted audits is also responsible for investigating complaints (Report at 8). However, NAI only reports publicly on findings of "material" non-compliance and does not report public on all complaints. The lack of transparency makes it impossible to determine if the complaint process is independent from other NAI activities, whether the public is fairly informed about complaints, or if the complaint process is straightforward. The vague concept of *material non-compliance* can hide a lot of transgressions. The complaint process, like the audit process, is neither independent nor transparent.

Issue 5: What was Audited for Compliance?

> From the Report:
>
> "The report includes a recommendation from the NAI staff "that all NAI members be required to report the domains they use for OBA purposes on a regular basis." Report at page 20.

If the NAI staff did not have a list of all domains used by member companies for online behavioral advertising (OBA) purposes on a regular basis, then how did it conduct a compliance review? A list of domains subject to the NAI rules seems to be a basic document for an audit. How could a complete compliance review possibly have been conducted without that list? Yet it appears that NAI conducted compliance reviews without a list for several years, and only in 2011 did it occur to anyone that a list of domains was a good idea. The recommendation together with a lack of any detail about what the NAI staff actually reviewed calls into question the scope and the bona fides of the work.

Issue 6: Misleading Standards

> From the Report:
>
> The NAI Code prohibits the use of non-PII or PII to create OBA segments specifically targeted at children under 13 without verifiable parental consent. Report at 22.
>
> "None of the evaluated members were found to create segments targeting children under 13." Report at page 22.

Comment: To a large extent, the NAI Code provision about children says nothing more than NAI members must comply with the law. It is not particularly meaningful if a self-regulatory code requires members to comply with a provision of a federal statute, in this case, the Children's Online Privacy Protection Act (COPPA). The report could just as well claim credit because NAI members drive their cars in the United States on the right side of the road.

COPPA includes other requirements for websites targeted at children under 13 that are not part of the NAI Code. It is not clear why the NAI Code chose to include one COPPA requirement but not the rest.

Further, the report offer no support for its conclusion that members are not targeting children under thirteen. How did NAI determine if activities were specifically targeted at children? The reader cannot tell because the report does not describe the standards used to make the judgment or the methodology used to verify compliance. A fair assessment would require a review of all targeting activities or a reasonable sample of targeting activities. The lack of details makes it difficult to evaluate the credibility of the conclusion.

> From the Report:
>
> "[T]he NAI Code has since 2008 forbidden members from using or allowing the use of, data collected for OBA for purposes such as employment, credit, and insurance eligibility." Report at pages 22-23.

Comment: Any company providing information for employment, credit, or insurance purposes would be subject to the Fair Credit Reporting Act (FCRA), a federal law that includes a long list of real fair information practices that are enforceable in multiple ways. No company engaged in OBA activities has any interest in being subject to the FCRA nor are their activities of the type that would normally fall under the FCRA. The NAI Code prohibition on using data for purposes such as employment, credit, and insurance eligibility is just as meaningless as if the NAI prohibited companies from collecting or disclosing information about zebras.

Issue 7: Security

> From the Report:

> "NAI staff reviewed member companies' ***descriptions*** of their security policies and protections, in order to establish that the member companies had conducted an appropriate evaluation of the technological, administrative, and physical protections for data subject to the NAI Code." Report at page 24 (emphasis added).

The compliance review apparently did not include a security audit, a test of security measures, or a verification that security was actually in place. It is not clear if the NAI staff had adequate technical expertise to conduct any type of security audit. The report states that NAI staff reviewed *descriptions* provided by member companies of their security policies and protections. This level of review is hardly a compliance audit and offers no meaningful reassurance to anyone. How a review of *descriptions* would allow anyone to determine if a company had actually conducted an evaluation is not clear. The essence of any compliance review is to determine independently if someone actually complies with a requirement, without simply taking their word for it.

#####

Document History

Version 1.1 First public release
Version 1.2 Minor edits and corrections