WORLD **PRIVACY** FORUM

February 25, 2011:
Comments on EASA Best Practice Recommendation on Online Behavioural Advertising.

Introduction

The World Privacy Forum submits these comments to the European Advertising Standards Alliance on its *Best Practice Recommendation on Online Behavioural Advertising*.

The World Privacy Forum (WPF) is a nonprofit, non-partisan 501 (C) (3) public interest research group. The organization is focused on conducting in-depth research, analysis, and consumer education in the area of privacy. It is the only privacy-focused public interest research group conducting independent, longitudinal work. The World Privacy Forum has had notable successes with its research, which has been groundbreaking and consistently ahead of trends. World Privacy Forum reports have documented important new areas, including medical identity theft. Areas of focus for the World Privacy Forum include health care, technology, and the financial sector. The Forum was founded in 2003 and works both nationally and internationally.

The WPF has long participated in the debate over self-regulation in consumer privacy issues. In the fall of 2007, the World Privacy Forum (WPF) released a report examining the effectiveness of the Network Advertising Initiative's (NAI) original principles that served as the basis of its self-regulatory agreement with the Federal Trade Commission (FTC). The report found that the NAI's principles had failed to effectively self-regulate the behavioral targeting sector because (1) the NAI ignored new business models, technologies and practices; (2) the NAI opt-out cookie and centralized opt-out page did not consistently honor a consumer's opt-out choices; (3) the NAI lacked a transparent and independent enforcement program; and (4) the NAI did not include a majority of industry groups in the behavioral advertising sector.[1] The NAI did not respond to this report, which we attach here in order to give context for the US experience in privacy self regulation.

[1] The 2007 WPF Report on the NAI Principles can be found here: http://www.worldprivacyforum.org/pdf/WPF_NAI_report_Nov2_2007fs.pdf.

Our comment proceeds in three parts. Properly implemented self-regulation can provide financial and reputational motivations for businesses to comply with consumer privacy interests while leaving businesses in control rather than lawmakers. But as proposed, the EASA standard is likely to repeat the history experienced in the United States with the NAI approach. First, we explain the need for strong privacy protection in the EASA standard so that it can gain legitimacy among consumers. Second, the US experience teaches that self-regulatory mechanisms for choice in this space have been largely ineffective, and that organizations have greatly increased their ability to track while not developing complementary technologies to persistently and reliably express consumer choice. The EASA approach is similarly narrow and does not address the long-noted failures of the NAI system in the US. Finally, the compliance measures as proposed will not effectively police the market. We make several recommendations for improvements.

Our prognosis for this endeavor is bleak. **The *Best Practice Recommendation* does not even invoke the protection of "privacy" as a policy goal.** Instead, the stated purpose of the document is to increase "consumer transparency and choice." Thus, normatively, the *Best Practice Recommendation* dismisses consumers' privacy concerns by not engaging them in any meaningful way. This is reflected in the proposed standard. Even those who exercise choice will be tracked pervasively for non-OBA purposes, which are so similar to OBA purposes that they cannot be defined without reference to each other. Because the system is based upon user awareness and opt out, those who are unaware of OBA privacy issues and do not opt out will have no privacy protection at all. Because it does not even embrace the protection of privacy as a policy goal, the *Best Practice Recommendation* stands upon a flawed foundation, and its recommendations reflect those foundational flaws.

Strong Privacy Protection is Vital to Successful OBA Self-regulation.

Privacy and data protection are fundamental rights under European law.[2] The protection of these rights is threatened because Online Behavioral Advertising (OBA) has created incentives for ubiquitous tracking of consumers.[3] Neelie Kroes, the vice president of EU Commission responsible for the digital agenda, urges for strong privacy protection in OBA and said,

> [U]sers should feel they have the effective possibility to choose whether they want to be tracked and profiled or not. Irrespective of their legality, any such practices are damaging –they damage the already fragile confidence in the online digital economy. Today only 12% of Europeans fully trust online transactions, so this sort of behaviour is a case of the industry 'shooting itself in the foot.' It is first and foremost the industry's responsibility to work to ensure that users have a genuine possibility to exercise personal choice. That is a matter of self-interest, in addition to the public interest it serves.[4]

Privacy protection and behavioral advertising are not mutually exclusive. In fact, consumers value both their privacy and the online services supported by advertising.[5] In addition, providing strong privacy protection is consistent with

---

[2] Neelie Kroes, *Towards more confidence and more value for European Digital Citizens*, European Roundtable on the Benefits of Online Advertising for Consumers 17 Sep., 2010, at 3, *available at* http://www.scribd.com/doc/37619863/kroesspeechsept17 ("Privacy and data protection have a particular value for Europeans: we consider them our fundamental rights and have put in place laws and regulations to protect them.").

[3] *See* Europa Press releases RAPID, *Citizens' privacy must become priority in digital age, says EU Commissioner Reding*, 14 Apr., 2009, *available at* http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/571 "Europeans must have the right to control how their personal information is used," said Viviane Reding, the EU's Commissioner for Information Society and Media. The Commission is concerned about the protection of this right when new technologies such as behavioral advertising make it easier to use, and misuse, personal information. She said, "European privacy rules are crystal clear: a person's information can only be used with their prior consent. We cannot give up this basic principle, and have all our exchanges monitored, surveyed and stored in exchange for a promise of 'more relevant' advertising! I will not shy away from taking action where an EU country falls short of this duty." Reding also warned, "the EU would take action where Member States fail to implement EU rules ensuring privacy and the need for a person's consent before processing his or her personal data."

[4] Kroes, *supra* note 2, at 4.

[5] *Id.* ("many Internet users value both their privacy and the online services supported by advertising. In other words – consumers want both, and it is our job to deliver that.").

profit interests of business.[6] This dynamic has been consistently noted in research, see for example, Colin Bennett's work in this area. He notes that "the protection of privacy fosters greater trust among consumers and is therefore a relatively inexpensive way to promote the image of corporate social responsibility. There is some empirical evidence that privacy protection may well be linked to higher levels of consumer trust."[7] Building confidence and trust in consumers is especially critical in OBA because new technologies raise more privacy concerns than others. Therefore, industry should proactively anticipate concerns and implement a robust self-regulation program.[8]

A robust self-regulation program with a high threshold of requirements allows participating businesses to distinguish themselves in a positive way. Instead of engaging in a "race to the bottom," in the context of a proper self-regulatory program, businesses can compete to known and documented benchmarks and standards. When consumers seek out businesses that comply with the self-regulatory requirements, those businesses engaging in this kind of positive competition can benefit.[9]

A successful self-regulation program has certain distinct characteristics. For example, the success of self-regulation in the print advertising industry can be attributed to the independence of the Advertising Standards Authority (ASA) from the industry it oversees. The composition of the ASA is two-thirds lay members and one-third independent individuals who bring useful inside experience from advertising. The ASA is responsible for interpreting and administering the British Codes of Advertising and Sales Promotion and monitors compliance with the Codes and investigates over 12,000 complaints a year. Other important features that contribute to its success include the ASA's monitoring and research program, the

---

[6] *See* COLIN BENNETT & CHARLES RAAB, THE GOVERNANCE OF PRIVACY: POLICY INSTRUMENTS IN GLOBAL PERSPECTIVE 159 (The MIT Press 2006) ("privacy codes work if strong privacy protection is consistent with the profit interests of business").
[7] *Id.* at 171-72.
[8] *See id.* at 172-73. ("New technologies tend to raise privacy fears more so than old ones . . . Most notably, as electronic commerce has penetrated the activities of every sector, there has been a corresponding need to anticipate privacy problems before they arise, and to assure consumers that their privacy is not at risk. Quite often the same practices as are conducted in the offline world can raise far greater fears when they are conducted online. The provision of credit-card information, for example, is generally less secure when a card is physically handed over the counter in a traditional retail store, than when it is transmitted via a secure server with strong encryption over the Internet. Nevertheless, the subjective perception of risk associated with a new technology can be a powerful motivation for companies to anticipate concerns and produce higher levels of self-regulation.").
[9] *See* National Consumer Council, *Models of self-regulation: An overview of models in business and the professions* 23 (November 2000), *available at* http://www.talkingcure.co.uk/articles/ncc_models_self_regulation.pdf.

publication of monthly Case Reports and an Annual Report and the sanctions of withdrawal of trading privileges including the denial of media space to offenders.[10] We note that the *Best Practice Recommendation* does not have rules to create norms consistent with this kind of a successful self-regulatory program.

A fragile self-regulation program with a low threshold of requirements has the opposite effect of a program like ASA's. Reputable businesses prefer non-involvement with weak programs because of the potential risks to brand image.[11] There are many signs that reveal a dysfunctional self-regulation program. For example, the Office of Fair Trading (OFT) was set up under the Fair Trading Act and has a duty to encourage trade associations to draw up and adopt consumer codes of practice. However, over time the ineffectiveness of codes of practice became increasingly apparent:

> Consumer awareness was sometimes very low, compliance was patchy, and some code sponsors seemed reluctant to impose meaningful penalties when things went wrong. In many areas complaint levels continued to be high. Traders were also concerned that their adherence to a code was not widely publicised and that costs of adherence put them at a competitive disadvantage. There was no effective means of distinguishing between effective codes and those primarily there for window dressing, nor any incentive to take on the ideas of interested parties in designing and enforcing the codes.[12]

The government has since developed a Consumer Codes Approval Scheme (CCAS) to address these issues and to encourage more rigorous and effective consumer codes. CCAS gives official approval to voluntary consumer codes of practice that meet criteria set by the OFT. The OFT in its documentation notes that "Businesses operating under an OFT approved code are licensed to use and display the OFT

---

[10] *Id.* at 31-32.

[11] *Id.* at 27.

[12] Office of Fair Trading, *Business Leadership in consumer protection: A discussion document on self regulation and industry-led compliance*, March 2009, at 30-31, *available at* http://www.oft.gov.uk/shared_oft/reports/consumer-policy/oft1058.pdf; National Consumer Council, *supra* note 9, at 26-27. In 1996, of the 38 trade associations responsible for overseeing 21 codes of practice, most reported few complaints and some said they had received no complaints. Independent lay involvement was rare and there was little evidence that commitments were being fulfilled or sanctions enforced. In 1998, the OFT published its own report and concluded that the codes had not met expectations: "Trade associations have difficulty in reconciling the roles of protecting members' interest with regulating standards of service . . . Trade associates face difficult disciplinary conflicts, especially when expulsion is the main sanction . . . There is a risk of a 'lowest common denominator' approach to setting standards."

Approved code logo which provides consumers a guarantee that the code has been rigorously checked and evaluated to ensure that it works in practice and deliver on its promises."[13]

OBA self regulation can learn from these examples. The OBA self-regulators assume dual roles to both represent the interest of their members and to protect privacy in furthering public interests. Self-regulators are responsible for implementing the program but they also have a vested interest in collecting and using personal information.[14] For this reason, the general public is often skeptical about the industry's commitment to the content of self-regulation and its enforcement.[15] This skepticism surrounding impartiality issues is heightened when the industry self-regulator, such as suggested by the *Best Practice Recommendation,* is responsible for enforcement and is involved in adjudicating disputes between consumers and its members.[16]

To alleviate this bias and gain consumers' confidence in OBA self-regulation, the content of the self-regulation "must be based on clear and intelligible statements of principles and measurable standards . . . which address real consumer concerns" and "[t]he rules should identify the intended outcome." Independence is vital to governance and enforcement, independence: like the print advertising industry, consumer, public interest and other independent representatives must be fully represented on the governing bodies and in any redress scheme that includes resolution of disputes between members and consumers. In addition, transparency and accountability are also important to provide confidence and trust in the program's effectiveness. A "clear, accessible and well-publicized complaints procedure" should be in place; compliance must be monitored and publicized in periodic reports and lastly, there must be "adequate, meaningful and commercially significant sanctions for non-observance."[17]

The next sections details the failure of the *Best Practice Recommendation* to meet these standards.

---

[13] Office of Fair Trading, *supra* note 12, at 31.
[14] *See* BENNETT & RAAB, *supra* note 6, at 171 ("the appetite for the collection and processing of greater quantities and increasingly more refined types of personal information is inherent in the logic of the capitalist enterprise.").
[15] National Consumer Council, *supra* note 9, at 23 ("there can be skepticism about the commitment of business interests to content of [self-] regulations and their enforcement."); BENNETT & RAAB, *supra* note 6, at 171 (The MIT Press 2006)
[16] *See* National Consumer Council, *supra* note 9, at 23.
[17] *Id.* at 51-52.

Illusory Protections are Created by the *Best Practice Recommendation*

The Best Practice Recommendation, as noted above, does not embrace consumer privacy as a policy goal. Instead, it advances the goals of consumer transparency and choice. Foundationally, securing consumer protection through notice is fraught with problems. Research in the US shows that consumers falsely believe that the mere presence of a privacy policy implies strong protections in law.[18] Thus a notice-based approach will be inherently misleading for a large number of consumers, who reasonably believe that notices labeled "privacy policy" must necessarily include a bundle of privacy rights.

Key to our objection to the *Best Practice Recommendation* is its narrow scope of regulating "Online Behavioural Advertising." It is narrow in the following ways:

- By limiting choice rights to OBA, it necessarily means that ad networks can still track consumers across multiple sites for purposes very similar to OBA. Thus, even if one opts out, the very same companies can collect the very same information on users, so long as they employ the data for different purposes.
- Users can be tracked behaviorally through multiple vectors, including through applications that are not browsers, such as chat, and through other platforms, such as video game consoles. Thus the definition is too narrow in limiting itself to tracking web behaviors.
- The US experience is illustrative here. After the NAI explicitly promised that all behavioral targeting technologies would be "subject to equivalent requirements for user notice and choice," the group failed to implement a universal and persistent opt-out mechanism that works just as reliably as all of tracking technologies currently in use by the industry. While HTML cookies are still the most widely used tracking technology available to the Industry, it is well-documented that after years of innovation, the industry has developed new technologies such as web beacons, XML, Silverlight and Flash cookies, browser fingerprints and HTML 5[19] in order to increase the persistency of their consumer tracking data.[20] By developing newer tracking technologies, the Industry now has the ability to track consumers on many different levels including across computers, Internet service providers and

[18] Joseph Turow et al., Americans Reject Tailored Advertising, September 2009, at 3, available at http://ssrn.com/abstract=1478214
[19] WPF Report on the NAI Principles, pg 19-28.
[20] Tanzina Vega, *Code That Tracks Users' Browsing Prompts Lawsuits*, NY TIMES, October 10, 2010, *available at* http://www.nytimes.com/2010/09/21/technology/21cookie.html.

even mobile devices.[21] It is not clear that the EASA standard will address the inherent narrowness of the industry opt-out mechanisms.
- Conceptually, the definition of OBA is extremely narrow, and thus the choice rights linked to it are not very meaningful.

An illustration of the last point appears in the definitions of "Ad Reporting' and "Ad Delivery." "Ad Reporting" and "Ad Delivery" involve tracking users over time and over multiple web sites for the purpose of delivering ads and engaging in analytics. These activities are so conceptually close to OBA, that EASA had to exclude OBA in order to define them. That is, these activities essentially cannot be differentiated from OBA. For the consumer, this means that the opt-out rights are largely illusory. What is being exempted if the consumer exercises choice is so narrow, that it cannot be defined without carving a small slice out of substantially similar tracking activities.

Additionally, the definition of *third party* requires some sharpening. It is common practice for publishers to give third party networks some ability to operate their sites by including JavaScript code that allows the third party network to install first party cookies on the publisher's site. The definition should clarify that *operate* refers to the day-to-day maintenance of the site's main content, in order to prevent third party advertising networks to claim that they technically "operate" publishers' sites.

We fundamentally disagree with opt-out approaches to OBA. Nevertheless, the opt-out approaches in the *Best Practice Recommendation* could be improved in several ways:

- As presented in Principle II, users will not have a single, unified mechanism to opt out. Instead, consumers will have to click on privacy policy links on every single network and opt out on a network-by-network basis. This is completely unworkable for consumers. Consider that a single website selling advertising may have OBA from several different networks, appearing as several different ads. The consumer would have to click on each notice associated with each advertisement. This would mean that consumers opting out on an advertising-heavy website would have to spend more time reading policies and opting out than interacting with the site's content.
- Third-party enhanced notices should provide a link to a centralized location where the consumer can make choices about all OBA, not just OBA from that particular advertising company.

---

[21] For example, a patent filed in 2005 – Network for matching an audience with deliverable content – boasts that users **can be re-associated with their profiles even if they have deleted cookies, and even if they are using different machines**. United States Patent Application 0050166233, Sections -0199-0200, 0212.

Embedded in the *Best Practices Recommendation* is a binary approach to privacy that can leave the consumer completely unprotected based upon choice or consent. For instance, Principle II calls for explicit consent to the adoption of technologies such as browser toolbars. Nothing in the document calls for these technologies to be cabined through privacy-by-design approaches. Thus, once explicit consent is gained, the consumer can be tracked on all websites, even if there are approaches to limit the privacy impact of such a decision (such as anonymization, truncation of URLs, limits on data retention, limits on secondary use) while still giving the consumer the benefit of the technology. This all or nothing approach fails to protect consumers regardless of the choices they take.

Much of the *Best Practices Recommendation* uses the exhortatory "should" instead of the mandatory "will not." For instance, in Principle II C, companies "should not" engage in techniques that circumvent user choice. Similarly, companies "should" take measures to address these practices and refer them to authorities. In these instance and others, the exhortatory language should be replaced with language indicating that compliance is mandatory, not optional.

Stronger Compliance and Enforcement Principles that build in Independent Oversight Will Benefit Consumer and Business Interests.

The three-phase complaint resolution mechanism in the EASA Best Practice Recommendation sets too high of a threshold for revocation of the B2B seal, does not mandate a structure with independent oversight, and provides inadequate statistical reporting requirements to allow the public to monitor compliance. Independent scrutiny of advertisers is necessary to ensure consumers are not harmed by violations of their online privacy. The EASA Best Practice Recommendation successfully recognizes the importance of oversight in a self-regulatory program with its "Compliance and Enforcement Guidance" section. Yet, the specific implementation of this principle does not adequately foster consumer trust to the benefit of compliant industry members. Below we describe how enforcement can be used as a tool to benefit businesses and consumers. Next, we advance five concrete steps to improve enforcement measures in the Best Practice Recommendation.

A. Enforcement is essential to building consumer trust in a self-regulatory organization.

Sufficient enforcement mechanisms are key to the efficacy of an online behavioral advertising self-regulatory program.[22] A well-functioning program rewards

[22] Federal Trade Commission, *Online Profiling: A Report to Congress, Part 2, Recommendations*, July 2000, http://www.ftc.gov/os/2000/07/onlineprofiling.htm, ("The bedrock of any effective self-regulatory or legislative scheme is enforcement. In a self-regulatory context, this means that nearly all industry members subject

members who comply with its principles and punishes those who do not to incentivize compliance. "[P]rotection of privacy fosters greater trust among consumers and is therefore a relatively inexpensive way to promote the image of corporate social responsibility."[23] Nonetheless, "[s]elf-regulation will always suffer from the perception that it is more symbolic than real because those who are responsible for implementation are those who have a vested interest in the processing of personal data."[24]

Businesses relinquish the ability to collect and use personal data in exchange for the image of corporate social responsibility embodied in the B2B seal. The B2B seal can be effective at minimizing the incentive to impermissibly process personal data,[25] but only insofar as consumers trust the seal. Rewarding compliance and punishing non-compliance strengthens the B2B seal. Failure to punish non-compliant companies sufficiently will contaminate the credibility of the B2B seal. This, in turn, will harm good actors by tarnishing their image of corporate social responsibility.

B. The EASA Best Practice Recommendation should strengthen its enforcement protocol.

The WPF urges improved compliance and enforcement procedures to ensure that the good actors in the online advertising industry receive the benefits of compliance they deserve. The three-phase complaint resolution mechanism in the EASA Best Practice Recommendation makes revocation of the B2B seal excessively difficult and requires inadequate reporting to permit the public to monitor compliance.

The three-phase process creates a bureaucratic thicket for consumers and at the same time inadequately tracks companies in violation of the Best Practices. In the first phase, "if the complaint is of substance . . . the main task of the SRO would be to

---

themselves to monitoring for compliance by an independent third party and to sanctions for non-compliance, which may include public reporting of violations or referral to the FTC."); J.J. Boddewyn, Advertising Self-Regulation: Private Government and Agent of Public Policy, 4 J. Public Policy & Marketing 129, 129 (1985) ("[O]btaining . . . 'good' advertising behavior requires that the following tasks be performed: (1) developing standards; (2) making them widely known and accepted; (3) advising advertisers beforehand about grey areas; (4) pre- or post-monitoring of compliance with the norms; (5) handling complaints from consumers and competitors, and (6) sanctioning "bad" behavior in violation of the standards, including the publicity of wrongdoings and wrongdoers.")

[23] Colin J. Bennett and Charles D. Raab, THE GOVERNANCE OF PRIVACY: POLICY INSTRUMENTS IN GLOBAL PERSPECTIVE, p. 171, The MIT Press.

[24] *Id.*

[25] *See Draft EASA Best Practice Recommendation*, at 33 ("In the UK, the IASH programme1 has proven that the removal of such a seal has significant effects on the market and is therefore an effective sanction, strong enough to enforce compliance.")

contact the company concerned and/or refer the complainant to the company."[26] At this point, the company works to resolve the issue with the consumer. Informal resolution is an understandable initial filter. But given that the consumer has made the extra effort to seek out a third party, the SRO can infer the consumer was displeased with the company's response and should investigate. At the very least, a public record should be kept at this point to note the frequency and nature of complaints linked to the identity of companies.

The second and third phases provide means to investigate and enforce the Best Practices, but the negative consequences for noncompliant companies are illusory. "Should a company continue to breach the rules on a *persistent and deliberate* basis, the SRO will apply other sanctions such as industry or relevant statutory referral"[27] (emphasis added). It is unclear how many violations are necessary to meet the standard of "persistent," and evidence necessary to demonstrate "deliberate" action would rarely, if ever, exist. Even if this nearly impossible burden is met, loss of the B2B seal is not guaranteed: "Industry referral *could* lead to other sanctions such as loss of the right to use an icon or seal"[28] (emphasis added). Consequences for noncompliance do not provide "adequate, meaningful and commercially significant sanctions for non-observance" that are critical to the success of a self-regulation program.[29]

To accommodate the shortcomings of an all-or-nothing seal, the Best Practices should clearly delineate the information it will publish on results of adjudication and complaints. If SROs publish the identities of companies involved in adjudication with the results of the adjudication, companies will have an incentive to comply as fully as possible even where violations do not rise to a level where the SROs should remove the B2B seal. Furthermore, if SROs conducted compliance audits that identify the performance of all members individually, it would reward companies that are vigilant toward consumer privacy. These steps will give SROs much needed independence to legitimize their regulatory role.

It is worth noting that SROs, which will presumably be industry-funded organizations, should be given specific instructions on what constitutes an adequate compliance audit. Compliance audits promised from Network Advertising Initiative, an online behavioral advertising self-regulatory organization in the United States, turned into ineffective advertiser-funded status updates. The most recent NAI compliance report featured conciliatory language and evaluated members' compliance in the aggregate without identifying the identities of violators or

---

[26] *Draft EASA Best Practice Recommendation*, at 31.
[27] *Id.*
[28] *Id.*
[29] *See* National Consumer Council, *Models of self-regulation: An overview of models in business and the professions* 53 (November 2000), *available at* http://www.talkingcure.co.uk/articles/ncc_models_self_regulation.pdf.

specifics of complaints.[30] Compliant businesses will only get value from participation in a self-regulation scheme if non-compliant businesses are independently and critically evaluated. As section 1 of this comment indicates, successful self-regulation in the print advertising industry was partially built on incorporating consumers, those working in the public interest, and other independent representatives in the redress scheme. The Best Practice Report would benefit from requiring SROs to do likewise.

These improvements to the EASA compliance and enforcement mechanisms would provide much needed structural mechanisms to incentivize consumer privacy. If the advertising industry does not create a self-regulatory program that acts as an unbiased watchdog fairly balancing business interests with consumer privacy, online advertisers in the European Union will suffer the same scrutiny that advertisers in the United States have faced in recent years.

The Network Advertising Initiative (NAI), the dominant self-regulatory body for online behavioral advertising in the United States, points to the "growing concern and awareness among consumers and lawmakers" about risk to consumer privacy with advertising technology.[31] The NAI has a record of a narrow scope of protection, limited membership, and inadequate enforcement mechanisms after having ample time over the last decade to correct its problems. In large part because of the failures of self-regulation, lawmakers in the United States are considering legislative regulation, which may entail public and private rights of action against advertisers.[32]

Properly implemented self regulation can provide financial and reputational motivations for businesses to comply with consumer privacy interests while leaving businesses in control rather than lawmakers. We urge improvements in the compliance and enforcement measures to ensure consumers get the privacy they have been promised and businesses get accolades, where deserved, for respecting that privacy. In conclusion, WPF urges EASA to update its Best Practice Recommendation to encourage SROs to:

> • Maintain detailed and publicly posted statistics on consumer complaints, the nature of the complaints, the targets of those complaints, and the frequency each company has been the subject of complaints;

---

[30] "2009 NAI Annual Compliance Report," *available at:* http://www.networkadvertising.org/managing/enforcement.asp

[31] "*An Industry at a crossroads – again,*" http://www.networkadvertising.org/networks/.

[32] *Do Not Track Me Online Act of 2011*, H.R. 654, 112th Cong. (2011); *The BEST PRACTICES Act*, H.R. 611, 112th Cong. (2011); *The BEST PRACTICES Act*, H.R. 611, 112th Cong. (2011).

• Investigate at an earlier stage in the complaint process in order to be more responsive to consumers;

• Report the results of adjudications and publish the identities of companies involved in adjudication with the results of the adjudication;

• Lower the threshold for removal of the B2B seal and set a clear standard for when it will be removed so that bad actors in the industry are not permitted to keep their seals; and

• Report the results of *independent*, self-initiated audits, and identify the performance of all members individually to reward companies that are vigilant toward consumer privacy.

Respectfully Submitted,

/s

Pam Dixon
Executive Director
World Privacy Forum
info2009@worldprivacyforum.org
2033 San Elijo Avenue, #402,
Cardiff by the Sea, CA 92007, USA

Filed on behalf of World Privacy Forum by the Samuelson Law, Technology & Public Policy Clinic at University of California, Berkeley School of Law by:

/s	/s	/s
Keyna Chow Clinic Student	Nicholas Petersen Clinic Student	Chris Jay Hoofnagle Senior Staff Attorney