Exhibit 1
Comparison of Two Leading UK and U.S. Industry Self-Regulatory Codes for Online Behavioural Advertising (OBA)

	Internet Advertising Bureau's (IAB) Good Practice Principles (IAB Principles) (U.K. trade association)	Network Advertising Initiative's (NAI) Self-Regulatory Code of Conduct NAI Code (U.S. trade association)
Self-regulatory code defines OBA?	Yes, OBA is advertising which is served based on data collected across single or multiple web domains owned or operated by different entities (non-affiliate companies) about a user over a period of time in order to create interest segments for the purposes of delivering online advertisements to that user.	Yes, OBA defined as any process used whereby data are collected across multiple web domains owned or operated by different entities (non-affiliate companies) to categorize likely consumer interest segments for use in advertising online.
Scope includes first party OBA? (advertising provided on a website the member owns and controls when no data is shared with third parties)	Yes	Yes, e.g., although the definition of OBA is limited to third-party OBA (see above), the code's notice requirements and some other parts of the code apply to both multi-site advertising practices and ad delivery & reporting by a single site.
Scope includes contextual advertising? (ad based on a single visit to a web page or search query with no data collection or retention)	No	Yes, although the definition of OBA excludes contextual advertising, contextual advertising is likely encompassed in ad delivery & reporting activities which are also covered by the code.
Scope includes sharing data with third parties?	Yes	Yes
Scope limited to personally identifiable data (PII)?	No	No
What type of notice is required for inclusion in OBA?	Each member and its contracted partners must provide clear and unambiguous notice that data are being collected for purpose of OBA.	Each member shall provide clear and conspicuous notice on its website that includes six specified types of information. Members also shall require websites with which they contract to post clear and conspicuous notice that includes four specified types of information.
What type of notice is required to use of PII?	Informed consent where required by law. PII defined as data that, by themselves or in conjunction with other data held by a member, uniquely identifies an individual offline.	Notice must include the types of PII and non-PII that will be merged by the member company, if any, and how any merged data will be used, including transfer to a third party. PII defined to include name, address, telephone number, email address, financial account number, government-issued identifier, and any other data used or intended to be used to identify, contact or precisely locate a person.
What level of consumer consent is required for inclusion of consumer in OBA?	The level of choice ranges from "opt out" to "opt in" with more robust consent required to use PII or sensitive personal data.	The level of choice ranges from "opt out" to "opt in" with the level of choice being commensurate with the increased privacy implications of data to be used.
What level of consent is required to collect sensitive data?	Explicit consent ("opt in") is required for the use of sensitive personal data, as defined and required by the EU Data Protection Directive (95/46/EC).	Opt in is required for the use of sensitive data (see definition of sensitive data below (not consistent with the EU Data Protection Directive).
Are data transfers to third parties (non-affiliate companies) restricted?	No, clear and unambiguous notice must be provided if data are being collected and used by third parties for the purpose of serving OBA and new contracts with third parties must require third party to give such notice that data are being collected and used by third parties for the purpose of serving OBA. Data Protection Directive generally restricts transfer of personal data.	Yes, third-party data sharing of PII is allowed only to companies under contract with the member that requires compliance with the NAI Code. If non-PII is transferred by a member, such contract must require compliance with the NAI Code for retroactive merger of non-PII with PII unless the non-PII is proprietary data of the third-party.
Must consumers grant explicit advance consent for third-party (non-affiliate) sharing of their data?	No, general notice and consent requirements apply and, in some cases, opt in consent is required (e.g., PII and sensitive data).	No, general notice and consent requirements apply (but see contractual requirements above).
What level of notice and consent is required to change a privacy policy to use previously collected data in manner materially different from promises made when the data was collected?	Member that provides OBA on its own domain(s) shall give, via its privacy policy, reasonable notice to users of any material change to its privacy policy with respect to its collection and use of data for the purposes of OBA.	Member's change of privacy policy with regard to PII and merger of PII with non-PII for OBA requires posting prior notice on a member's website. Material changes in company's privacy policy apply only prospectively unless the consumer opts-in to allow collected information to be covered by the new policy.

Comparison of Industry Self-Regulatory Codes		
	IAB Principles (U.K.)	**NAI Code (U.S.)**
Is sensitive data defined?	Yes, as defined by EU's Data Protection Directive (95/46/EC).	Yes, it includes social security numbers or other government-issued identifiers, insurance plan numbers, financial account numbers, information that describes the precise real-time geographic location of an individual and precise information about past, present, or potential future health or medical conditions or treatments, including genetic, genomic and family medical history.
Is geographical location data treated as sensitive data?	No, but see E-Privacy Directive.	Yes, includes precise real-time geographic location of an individual derived through location based services.
Is the creation of sensitive marketing segments (group profiles) for OBA purposes limited?	Yes, OBA segments intended for the sole purpose of targeting children under the age of 13 years are prohibited. Member discretion on creating other segments is permitted to be guided by the over-riding objective of maintaining user trust.	Yes, use of non-PII or PII to create an OBA segment specifically targeting children under 13 is prohibited without verifiable parental consent; OBA segments can only be used for marketing purposes. No limits on creation or use of other sensitive marketing segments.
Does the code require OBA to use reliable sources for data?	No, but data accuracy for PII is a principle of the EU's Data Protection Directive (95/46/EC).	Yes, requires members to make reasonable efforts to ensure they are obtaining data for OBA, multi-site advertising and ad delivery and reporting from reliable sources.
What limits are there on data retention?	Not specified, but data retention is regulated under the principles of the EU's Data Protection Directive (95/46/EC).	Members should retain data collected and used for covered activities only so long as necessary to fulfill a legitimate business need or as required by law.
What level of security precautions is required?	Not specified, but data security is required under the principles of the EU's Data Protection Directive (95/46/EC).	Reasonable security for collection, transfer or storing data.
Is the code binding?	Yes, prospectively binding on signatory members of the IAB.	Yes, on all signatory members of the NAI.
Are enforcement mechanisms provided?	Yes, includes company self-certifications and requirement to publicly acknowledge commitment to the code's principles (attestations). Must have complaint mechanisms to handle complaints and inquiries. Users may bring complaints to the OBA Board.	Yes, include pre-certifications for new members, public representation by members of compliance with each aspect of code (attestations), annual compliance reviews by NAI designee and consumer complaint mechanisms. Credible unresolved consumer complaint may also justify a compliance review.
Are there penalties for noncompliance with the code?	None stated.	Penalties that could be imposed for a finding of non-compliance to be posted on NAI's website and include referral of the matter to the FTC.
Does the code apply to data collected outside the traditional website context that is used for OBA, for example demographic data?	No, but see EU Data Protection Directive and E-Privacy Directive.	Yes, e.g., retrospective merger of PII with previously collected non-PII for OBA purposes requires opt in consent when it is first used online.
Is behavioral advertising of mobile customers expressly covered?	No	No
Does the code give consumers meaningful access to information about individually-applied profiles used to generate targeted advertising?	No, however access to personal data is required by the Data Protection Directive that applies to all personal data processing (but it is not clear that individually-applied profiles are personal data under this Directive).	No, members must only be provided with reasonable access to PII retained by the member for OBI and "other information that is associated with PII (it is not clear that individually-applied profiles are covered by this rule).
Does the code prohibit unfair or discriminatory application of profiling to consumers?	No, but see discussion above on sensitive marketing segments.	No, but see discussion above on sensitive marketing segments.
Relationship of code to applicable laws and regulations.	This code expressly recognizes that it complements and in some cases supplements application of the UK's legal framework. The EU's Data Protection Directive (95/46/EC) and other applicable law (e.g., the Privacy and Electronic Communications Regulations) remain applicable for members located in the UK.	Members shall adhere to all laws applicable to their businesses and where those laws exceed or conflict with the requirement of this self-regulatory code, shall abide by applicable law. Where the requirements of the self-regulatory code exceed applicable law, members shall conform to the higher standards imposed by this code unless it would be contrary to applicable law.