January 10, 2001

Ms. Lynne Ross
Executive Director
National Association of Attorneys General
750 1st Street, NE, Suite 110
Washington DC 20002

Re: Draft NAAG Privacy Principles and Background 12/11/00

Dear Ms. Ross:

The NetCoalition appreciates the opportunity to comment on the December 11th draft of NAAG's Privacy Principles (hereafter "the draft" or "the draft Principles"), and to submit suggested modifications regarding the draft's treatment of *preemption*, *opt-in* and regulation of *non-individually identifiable information*.

The NetCoalition is the first public policy organization comprised of members whose primary business is purely Internet-based. Our members include Yahoo!, America Online, Terra Lycos, Inktomi, Excite@Home, and DoubleClick. We represent innovators in e-commerce and interactive services, advertising and infrastructure, person-to-person trading, and search and navigation systems who have a critical stake in policy developments affecting the Internet.

Our members are committed to protecting the privacy of Internet users' online experiences. We believe that privacy is fundamental to the continued growth of the Internet, and that consumer trust is essential. That is why the NetCoalition has engaged in an aggressive public education and web advertising campaign on privacy, and our CEOs wrote the CEOs of the 400 leading online sites to urge them to adopt robust privacy policies addressing notice, choice, access and security.

The NetCoalition appreciates the Committee's openness to receiving input from the public, and the evident good intentions and consideration that have gone into the draft Principles. However, we have three over-arching concerns with the conclusions in the draft:

1. In opposing preemption of state substantive privacy standards (as opposed to state enforcement authority), the draft does not realistically account for the inherently interstate¾ and indeed, international¾ character of the Internet.

2. In supporting an across-the-board opt-in standard for privacy, the draft overlooks long-standing differences in treatment between sensitive and non-sensitive information in ways that would have a very negative effect on e-commerce.

3. In advocating an opt-out standard for information that is not even individually identifiable, the draft completely departs from precedent in U.S. privacy law and would burden even the most privacy-friendly websites in circumstances that do not implicate privacy issues.

Online privacy issues are very complicated, and should be addressed only after serious dialog between policymaker, industry and Internet users. The NetCoalition is still evaluating the appropriate response to online privacy problems and whether legislation is needed at this time to supplement the State Attorneys General's ("AGs") and FTC's existing unfair and deceptive practice authority. However, with the changes outlined above, the NAAG Principles would be a thoughtful and influential contribution to the debate on online privacy.

1. The Principles Should Recommend Limited Preemption

In order to make the Principles viable for the Internet, we urge the drafters to revise them to propose a uniform national standard for Internet privacy, enforced by both federal officials and the State Attorneys General. This is precisely the approach taken by the only federal online privacy statute, the Children's Online Privacy Protection Act ("COPPA"), and is the only one that makes sense for the Internet.

Internet business arrangements defy a state-by-state approach to privacy, even if regulation were premised upon the state in which the receiving computer server were located. The Internet portal business provides a good example. Portal businesses typically depend upon user visits to the portal site, which may be "mirrored" on computer servers in multiple states to reduce network congestion. Portals typically keep logs of user visits¾retained for security purposes¾and may store them in another state. Portals are supported in part by advertising supplied by ad server companies, which are usually located in a different state. Finally, portals link to and sometimes partner with other websites, whose businesses and computer servers are often located in yet another state. All of this contributes to the seamless availability of content that consumers find extremely useful and valuable. As a result, a user's visit to a portal can involve limited amounts of data flowing to any of a large array of states. If even a few of these states had different online privacy requirements, compliance with these requirements would be hopelessly complicated.

We can well understand the reluctance of state law enforcement officials to recommend federal preemption of state substantive standards. However, a uniform national online privacy standard would fully preserve states' abilities to protect their citizens through enforcement of either national substantive privacy standards or traditional unfair and deceptive practice laws. Moreover, states have not yet adopted Internet privacy laws other than spam laws and, as discussed below, there is serious doubt whether such laws would even pass constitutional muster under the Commerce Clause.

The inherently interstate nature of Internet communications makes it essential that any legislative standards on Internet privacy be established on a nationwide basis. To start with the first of the Fair Information Practices, notice, a single national notice requirement is the only way to legislate in this area. Every website in the U.S. is accessible to citizens in every state. Without preemption, every company within reach of a state long arm statute would need to conform to the notice requirements of every one of those states that chose to legislate on the subject matter. If states proceed to adopt differing online privacy notice standards that conflict in some respect, websites would be unable to comply without engaging in *more* data collection (asking every user what state they are from) and posting a separate privacy notice for each state. This exercise would in no way advance privacy, would place a regulatory roadblock to user access to websites, and would impose heavy legal compliance costs on free websites.

Similar serious problems would arise in applying any of the other Fair Information Practices identified in the draft Principles under differing state laws. Internet companies would be confronted with requirements to conform to multiple choice, access, security and enforcement standards based upon the state of residence of the consumer, which those sites in many cases would not even know.

Moreover, attempts to impose state-by-state regulation of Internet privacy are most likely unconstitutional for violating the dormant Commerce Clause. Courts have repeatedly struck down state efforts to regulate activities and content on out-of-state websites, and have made clear that the Commerce Clause does not permit imposition of inconsistent requirements. See, e.g., ACLU v. Johnson, 194 F.3d 1149, 1162-63 (10th Cir. 1999) (noting the danger that "a single actor might be subject to haphazard, uncoordinated, and even outright inconsistent regulation by states); ACLU v. Pataki, 969 F. Supp. 169, 181 (S.D.N.Y. 1997) (noting that inconsistent state regulation "could paralyze the development of the Internet altogether").

States imposing different substantive requirements for website privacy would likely leave websites no choice but to comply with the most restrictive state rule applicable to each aspect of online privacy. This would raise not only dormant Commerce Clause, but also serious First Amendment problems. See ACLU v. Reno, 217 F.3d 162, 173-77 (3d Cir. 2000) (federal harmful-to-minors law is unconstitutionally overbroad because it subjects websites to the "community standards" of different communities).

For all these reasons, the Principles should be revised to recommend uniform national standard for Internet privacy enforceable by federal authorities and State Attorneys General, supplemented by continuing state authority with regard to unfair and deceptive trade practices.

2. The Principles Should Change Default Opt-in Rule to Default Opt-out Rule

The draft Principles indicate that the use of or disclosure of individually identifiable information for purposes "other than the purpose for which the information was obtained" should require an "opt-in." This proposed recommendation departs sharply from the scope of opt-in requirements under existing federal privacy laws, where it has been reserved for the most

sensitive types of information that could have a significant adverse effect on the consumer. An opt-in requirement for information regarding individual shopping and content preferences would significantly impair consumer choice on the Internet by limiting the rich array of free, innovative offerings that have been critical to the success of the Internet.

The draft recognizes that sensitive and non-sensitive information have been, and should be, treated differently under U.S. privacy laws. However, it incorrectly classifies factors such as income and purchasing habits as sensitive information. Draft Principles at 14. Federal privacy law reserves opt-in rules for truly sensitive uses of information, such as some uses of individually identifiable medical, children's and credit information. It almost always applies an opt-out standard to private sector uses and disclosures of data on income and purchasing patterns. In fact, even the Clinton Administration's recent health care privacy regulations allow use of highly sensitive medical information for marketing purposes subject to an opt-out following receipt of a general standard patient consent form. See 45 C.F.R. § 164.514(e).

The draft assumes that opt-out will be ineffective because the choice to opt-out is "buried in the fine print" and is burdensome to consumers. In fact, the assumption that there is a sharp dichotomy between opt-in and opt-out is misplaced. Robust notice and meaningful choice for consumers is what Internet consumers want and need to control their privacy online. Policymaking on privacy should ensure consumer choice, but provide enough flexibility so that consumers and businesses can decide what kind of choice is appropriate in each circumstance, and allow for technological innovations that will empower consumers to protect themselves.

The draft's concern about the risk of deficient opt-out notices can simply be addressed by a requirement that notice be clear and conspicuous. It does not require the extraordinary imposition of an opt-in requirement. Moreover, as the draft appears to acknowledge, the Internet is uniquely well-suited to offer customers a simple means of opting out. They can simply e-mail the Internet company to ask to be removed from a list. In fact, most leading Internet sites offer consumers convenient notice and choice options. The NetCoalition and its members have devoted significant efforts to educating consumers about such capabilities.

A well-crafted opt-out approach protects consumer privacy while permitting the seamless offerings of the Internet. Information is utilized by Internet sites in ways desired by consumers and for advertising that is in large part responsible for the volumes of free content and other inexpensive offerings available on the Internet. Opt-out allows the benefits of personalization and responsible use of non-sensitive information to continue.

By comparison, an opt-in system would restrict the use of information upon which much of the content and services on the Internet depend. An opt-in approach would inhibit the growth of the online medium and reduce competition. It imposes significantly higher costs than an opt-out approach, with very different economic implications. Such costs would limit the viability of business models, significantly reduce the amount of free and inexpensive content and services available on the Internet, and ultimately increase costs for consumers. An opt-in would result in a burden on consumers who expect the personalization with respect to the services and interests of consumers that is possible on the Internet.

An onerous opt-in regime would also make it harder for new entrants to establish a foothold in the market. Less established players have a much harder time obtaining customer consents. Internet innovators are just beginning to scratch the surface in developing and offering innovative services providing new conveniences to consumers. An opt-in risks curtailing services consumers have yet to experience. Moreover, an opt-in rule might work very much to the advantage of established monopolists and other gatekeepers, who have closer relationships with consumers, and are better positioned to obtain consents as a condition of receiving service.

3. The Principles Should Not Recommend Regulation of Non-individually Identifiable Information

The draft Principles depart most sharply from existing privacy law in their suggestion (at p.14) that aggregate, non-individually identifiable ("non-identifiable") information collected in the marketplace be treated as private and subject to an opt-out rule. Such a requirement would be unprecedented, and would seriously interfere with the operation of websites in circumstances that have no privacy implications whatsoever.

No federal law has ever considered non-identifiable information collected in a commercial setting as private. Indeed, federal laws are careful to create complete exceptions for this type of non-identifiable information. This is true, for example, of COPPA, the only federal online privacy law, which chose not include in its definition of "personal information" information that does not permit the contacting of a "specific individual." 15 U.S.C. § 6502(8)(F). Similarly, the Cable Communications Privacy Act, specifically exempts aggregate information from the reach of that statute. 47 U.S.C. § 551(a)(2)(A). Even in the context of medical privacy, the Clinton Administration's Health care privacy regulations apply only to "individually identifiable health information" protected health information" limit the scope of the regulations have exempted "de-identified information" from the regulations' opt-in requirement. 45 C.F.R. § 164.501 (definition of "protected health information").

This rule would unfairly burden the Internet because online sites must all collect anonymous information on visitors to their sites for security purposes to detect hacking, as well as to improve the content of their sites, and to measure traffic on the site in an effort to make it profitable. Providing for opt outs from these and other non-identifiable uses of information would harm the ability of free, privacy-friendly websites to function, and would not materially advance privacy.

The draft's proposal to regulate non-identifiable information may stem from concern that the information might later be merged with identifiable data. Regulating non-identifiable information is not necessary to address this concern. If this were to occur without being disclosed in a site's privacy policies, the company in question would need to provide appropriate notice and an opt-out opportunity to avoid liability for a deceptive trade practice.

4. Conclusion

The NetCoalition appreciates your consideration of our views regarding: (1) providing for limited preemption in the draft principles; (2) recommending an opt-out rather than opt-in rule for non-sensitive information such as customer income and shopping preferences; and (3) eliminating any suggestion that non-individually identifiable information be subject to an opt-out rule.

We would be happy to answer any questions you may have, and hope to work with you further on this important issue for the future of the Internet.

Sincerely,

Daniel R. Ebert
Executive Director