Comments on the NAAG Draft Privacy Principles

The Direct Marketing Association ("The DMA") and the Internet Alliance ("IA") appreciate this opportunity to comment on the December 11, 2000 draft of the National Association of Attorneys General ("NAAG") Privacy Principles & Background ("Draft"). The DMA is the largest trade association for businesses interested in direct, database, interactive marketing, and electronic commerce. IA, a subsidiary of The DMA, is the premier organization of Internet policy professionals representing the Internet online industry on the state, federal and international levels.

The DMA and IA believe that there exists a significant role for state attorneys general to play in protecting their citizens with respect to privacy and on the Internet. If it is determined that legislation is needed in this area, The DMA and IA believe it should be only at the Federal level and it should be limited to notice and choice. It is critical to the growth of commerce and the protection of consumers to have a single Federal standard that preempts the creation of differing state privacy standards but which permits state enforcement of the Federal standard.

We conclude, therefore, that the approach taken in the Draft has serious flaws and applies an antiquated approach to privacy and consumer protection that is ill-suited for the information age, and ultimately is not in the best interest of consumers. In short, the NAAG draft risks unduly burdening the free flow of beneficial commerce and ideas.

As FTC Chairman Robert Pitofsky frequently says, "The Internet is a profoundly positive consumer development." These benefits exist because of the multitude of offerings and free flow of information that result from the Internet. The development of the Internet has resulted in an astounding choice in products and services available from around the world at the click of a mouse. Likewise, consumers' ability to obtain information about the merchants with whom they choose do business is unprecedented. The DMA believes that a privacy framework for the information age should reflect the characteristics of the medium—it must be global in nature, it must be flexible enough to allow for constant and rapid technological changes, and it

must not impose significant new costs that could become barriers to entry. The over-regulatory approach proposed by the draft threatens to impinge on these characteristics.

Instead, the NAAG approach to privacy should recognize the complexity of these issues and allow for flexibility rather than impose unnecessary regulatory burdens. A strong stance against any type of federal preemption fails to account for the unique characteristics of privacy in the information age. During the past few years, extraordinary progress and innovation have been made in connection with policy approaches to consumer protection, including privacy protection, on the Internet. They include self-regulation, safe harbors, unique approaches to preemption with state attorney general enforcement, and technological empowerment tools and in some cases, Federal legislation. We believe these concepts should be incorporated into NAAG's draft. Additionally, the NAAG approach should allow for consumer choice, rather than mandate "opt-in." Preemption, new approaches to privacy protection, and consumer choice are discussed in more detail below.

I. The NAAG Policy Framework Should Reflect the Revolutionary Nature of the Information Age and the Internet

The underlying premise of the NAAG proposal to oppose federal preemption of state law is that privacy in the information age is no different than other forms of commerce and that the state's ability to legislate must be preserved when considered in the context of the Internet. This premise is simply not true. The current level of international commerce by consumers and the ability to instantly exchange information across boundaries fostered by advances in information technology is unprecedented.

Differing state regulatory standards for the Internet could have the effect of eliminating the inherently global characteristics of the Internet, which are the features of the Internet that in large part are responsible for its extraordinary success. It would be impossible for businesses to comply simultaneously with inconsistent local privacy laws in multiple jurisdictions where their

customers may be located.[1] If businesses were required to comply with the different laws of the 50 states, it would be a tremendous burden on the Internet and could have the result of limiting Internet business offerings. A patchwork of state privacy laws, particularly as they affect the Internet, may ultimately be found unconstitutional. The Supreme Court has suggested that the aggregate cost of complying with multiple regulations, a burden that is uniquely placed on interstate businesses, must be taken into account in determining the validity of individual state regulations¾ even if the difference among the various states' rules is not so dramatic as to render them contradictory, and indeed even if the rules are all identical.[2]

Constitutional challenges to state legislation affecting the Internet based on the "dormant" Commerce Clause are occurring with increasing frequency. In these cases, the courts have repeatedly struck down state legislation burdening the operation of the Internet because it violates the dormant Commerce Clause of the U.S. Constitution. In ACLU v. Johnson, the court stated that "the unique nature of the Internet highlights the likelihood that a single actor might be subject to haphazard, uncoordinated, and even outright inconsistent regulation by states that the actor never intended to reach and possibly was unaware were being accessed. Typically, states' jurisdictional limits are related to geography; geography, however, is a virtually meaningless construct on the Internet." ACLU v. Johnson, 194 F.3d 1149, 1161-62 (10th Cir. 1999) (striking down state harmful-to-minors law).

Likewise, in American Libraries Ass'n v. Pataki, 969 F. Supp. 160, 177 (S.D.N.Y. 1997), the court struck down a New York statute prohibiting the depiction of sexually related material on the Internet that was harmful to minors. The court stated, "The conclusion that the Act must

---

[1] For example, in the widely publicized recent LICRA v. Yahoo case, a French court is asserting jurisdiction over servers in the U.S. for content prohibited in France. While we may abhor such speech in the United States, it is protected by the First Amendment. Requiring companies to comply with the laws and standards of numerous jurisdictions as the French are attempting to do would be devastating to the quality and content of Internet offerings to consumers.

apply to interstate as well as intrastate communications receives perhaps its strongest support from the nature of the Internet itself. The Internet is wholly insensitive to geographic distinctions." Id. at 170. The court went on to note with respect to the dormant Commerce Clause, "The courts have long recognized that certain types of commerce demand consistent treatment and are therefore susceptible to regulation only on a national level. The Internet represents one of these areas; effective regulation will require national and more likely global cooperation. Regulation by any single state can only result in chaos, because at least some states will likely enact laws subjecting Internet users to conflicting obligations. Without the limitation imposed by the Commerce Clause, these inconsistent regulatory schemes could paralyze the development of the Internet altogether." Id. at 181.

There is, however, an important role for state-based enforcement of national standards. The recently enacted Children's Online Privacy Protection Act ("COPPA") provides for state attorneys' general enforcement of Federal standards. The DMA believes that it is of critical importance to consumers and business to have a single standard at the national level. It is appropriate for state attorneys general to be able to enforce that standard, but it would not be appropriate as suggested by your draft to have 50 different state standards.

II. Alternative Forms of Online Privacy Protection

In the past few years, a framework for regulating privacy has been developing that takes into account the rapidly advancing, global characteristics of the Internet. Self-regulation, safe harbors, state attorney general enforcement of Federal law, and consumer empowerment technologies all offer more effective approaches to privacy protection for consumers than that proposed by NAAG. While these approaches are early in their development, they have been

---

(footnote continued from previous page)

[2] Laurence H. Tribe, American Constitutional Law, Third Edition, New York, New York, Foundation Press, 2000.

successful. NAAG should evaluate these developments and incorporate them into the NAAG draft. We describe them here.

Self-Regulation

Companies at the forefront of the information age are responding to the challenges posed by this complex issue. These companies have devoted significant resources to developing well-planned, well-intentioned, and effective self-regulatory privacy principles. Their experience allow them to best understand how to address consumer concerns without hindering development of the medium.

A recent FTC report states that all of the 100 most popular sites on the Internet post privacy notices. Moreover, since the development of self-regulatory principles for Internet privacy, 88% of all sites post privacy notices¾ up from 66% in 1999 and 14% in 1998. Another significant development is the rapid adoption of The Direct Marketing Association's Privacy Promise and the BBB*OnLine* and TRUSTe privacy seal programs with enforcement provisions. More than 2,500 companies have signed on to the Privacy Promise, which will empower consumers with notice and choice concerning transfer of their information to third parties. Likewise, BBB*OnLine* and TRUSTe have quickly signed up thousands of participants. To the extent that companies post policies and do not follow them, the Federal Trade Commission and state attorneys general can prosecute these sites for deceptive practices.

Safe Harbor

The use of safe harbor provisions allows businesses to comply with a single substantive privacy standard and thus be deemed compliant with the laws of multiple jurisdictions. Safe harbor provisions have been included in both the recently implemented Children's Online Privacy Protection Act ("COPPA") and the European Union Directive on Data Protection. Under a safe harbor provision, entities that follow substantive safe harbor guidelines are deemed to be in compliance with the law's general substantive guidelines. Safe harbors act as bridges between two different approaches to the same consumer protection issues.

Attorney General Enforcement of Federal Standards

Likewise, another approach is Federal legislation setting a uniform Federal standard that can be enforced by state attorneys general. The importance of retaining an attorney general's ability to protect the consumers of his or her state, while maintaining a national standard is clearly reflected in COPPA, which codifies the right of states to enforce federal law. Section 6504(a)(1) provides that, where an attorney general has reason to believe that his or her residents' interests have been threatened or adversely affected by the acts of a third party, the state may file a civil lawsuit for specified reasons, including to enforce compliance with the COPPA regulation.

Consumer Empowerment Technologies

Consumer empowerment technologies, where consumers located anywhere around the globe can set their own preferences, will allow for robust choice for the individual consumer. One technology initiative aimed at empowering consumers is the Platform for Privacy Principles, or "P3P." This initiative of the World Wide Web Consortium utilizes a "negotiation" approach to the protection of privacy. A broad coalition of information providers, advertising and marketing specialists, software developers, credit services, telecommunications companies, and consumer and online advocates have worked together on this effort, which provides a technological solution that will protect privacy in a manner that can be international.

This user empowerment technology will be built into the next generation of Internet browsers. It allows a user to agree to, modify, or reject the privacy practices of a web site and thus be fully informed in advance of interacting with or disclosing information to a site. This approach will enable webmasters to classify information practices on their sites according to a uniform classification system, and enable consumers to "set" personal privacy preferences within their web browsers. When a consumer visits a web site that collects information from visitors, the web site will collect and use personal information of the consumer according to the consumer's pre-set preferences.

III. The NAAG Draft Should Allow for Choice and Not Be Limited to Opt-In

The type of choice given to consumers in Federal privacy law should be opt-out, not opt-in (although opt-in may be appropriate with extremely sensitive data such as health records). The opt-out rule has been widely accepted by Congress. It has proven to create the proper balance between protecting privacy and allowing the benefits of use of information to continue. Opt-in and opt-out both give consumers choice about whether their information is used. Neither approach provides individuals with greater or lesser protection than the other because in either instance the consumer's preference is honored. In contrast to opt-out, however, an opt-in approach imposes significantly higher costs, with very different economic and legal implications. The additional costs associated with an opt-in regime are measured not only in economic terms (higher prices and lost opportunities), but also in additional burdens on consumers and businesses, and potential infringement upon First Amendment rights.[3]

An opt-out approach sets the default rule to "free information flow," while affording more privacy-sensitive individuals the opportunity to prevent the use of their information. By comparison, an opt-in system sets the default rule to "no information flow," thus restricting the use of information to further the growth of the online medium. The costs associated with opt-in are costs that society has determined at times are appropriate in the case of the most sensitive information, such as personal health information, but not for marketing information.

Both the opt-in and opt-out approaches give consumers choice about whether their information is used. An opt-in approach, however, would serve to inhibit the growth of the online medium and reduce competition. Even the recently released health care privacy regulations of the Department of Health and Human Services permit health care providers operating under a general consent to use health care information to market to their own patients subject to an opt-out. This approach was adopted because of the recognition of the importance of describing new

treatments, medicines, and offerings to patients. See 45 C.F.R. § 164.514. Adoption of an opt-in approach to privacy for marketing purposes would make it more difficult for new and often more innovative companies to enter and compete in the online environment.

More onerous opt-in regulation would also make it harder for new entrants to establish a foothold in the market, and would likely reduce the availability of "free" content on the Web. It also would inhibit companies' ability to tailor their marketing efforts or improve customer service and customer relations efforts. An opt-in requirement risks shoehorning the Internet into an inflexible regulatory regime, stifling its potential growth and hindering innovation. In addition, opt-in would impose significant costs on businesses for reprogramming their computer systems to an opt-in model, archiving consents, and matching consents to the activities to which they apply.

An opt-in approach would also reduce the completeness and accuracy of information and may have the effect of increasing fraud. Such an approach would serve to undermine identity verification efforts in connection with rolling out new online services, especially e-commerce services. In contrast, opt-out enables companies to authenticate customers and verify information, as well as assisting in counteracting fraud while preserving privacy protections. An opt-in regime thus could have the effect of raising prices for products and services because competition would be reduced while increasing fraud-related and marketing costs.

Conclusion

There exists significant opportunity for NAAG to revise its draft privacy principles so as to propose policies that reflect the information age, ultimately providing better protections and offerings to consumers. The Draft, however, would apply an outmoded regulatory approach,

---

(footnote continued from previous page)

[3] See U.S. West, Inc. v. FCC, 182 F.3d 1224 (10th Cir. 1999), cert. denied, 120 S. Ct. 2215

(footnote continued to next page)

which could have the effect of eliminating the inherently global characteristics of the Internet, placing tremendous burdens on businesses and imposing barriers to entry, thus reducing business offerings over the Internet. Similarly, NAAG's "opt-in" principle may violate the First Amendment. NAAG's revised proposal should instead reflect more effective approaches to consumer privacy protection that promote the revolutionary nature and characteristics of the Internet and the information age. Such approaches include self-regulation, safe harbors, attorney general enforcement of federal standards, and consumer empowerment technologies. Likewise, consumer "opt-out" as opposed to "opt-in" should be incorporated into the draft to allow for the free flow of information.

* * *

The DMA represents more than 4,600 companies in the United States and 54 other nations. Founded in 1917, its members include direct mailers and direct marketers from 50 different industry segments, as well as the non-profit sector. Included are catalogers, financial services, book and magazine publishers, retail stores, industrial manufacturers, Internet-based businesses and a host of other segments, as well as the service industries that support them.

The DMA member companies and their customers have a major stake in "information age" and the success of electronic commerce, and are among those most likely to benefit immediately from its growth. In addition to the 4600 companies that are DMA members, The DMA's leadership in the Internet and electronic commerce areas is present through its subsidiaries the Internet Alliance and the Association for Interactive Media. Accordingly, The DMA has been working diligently in helping define an appropriate policy framework for the Internet and its World Wide Web.

(footnote continued from previous page)
(2000).

IA, through public policy, advocacy, consumer outreach and strategic alliances, is building the confidence and trust necessary for the Internet to become the global mass market medium of the 21st century. Current members include: @Once, 24/7Media, America Online, BMG Entertainment North America, Citibank, the Council of Better Business Bureaus, Cox Interactive Media, Juno Online Services, IBM, Microsoft, Privada, Prodigy Communications, UUNet, and Verizon.