Comcast Position Paper for Submission to the W3C Workshop on Web Tracking and User Privacy[1]

Protecting the privacy of consumer information transported over the Internet deserves the high-priority attention of all stakeholders in the emerging marketplace of online communications and commerce. Consumers are rightly concerned that the personal information they provide over the Internet may be collated, gathered, tracked and distributed in myriad ways so that far too many persons and entities will know far too much about them. Cable operators and programmers not only understand these concerns but are committed to protecting the privacy of their customers. Comcast, as a member of the cable industry, has actively participated in the privacy policy discussion with federal regulatory agencies, legislators, industry groups, and public interest groups. For Comcast, the upcoming W3C Workshop provides a critical opportunity to work with stakeholders and continue to advance the privacy policy conversation.

For cable operators like Comcast, the privacy of their customers is not a new concern. Since long before they began offering broadband service, cable operators have been taking steps to protect customers of their cable television service against any undesired disclosure of their personally identifiable information ("PII") and their purchasing and viewing decisions. Since 1984, such measures have been required by federal law. But they're also a business imperative – especially in today's competitive broadband marketplace. For all the services that cable operators now offer – video, broadband and telephone – consumers have choices. Moreover, more and more consumers are now purchasing all these services from a single provider, so that the costs of losing a customer to a competitive provider are compounded. In other words, cable operators have singularly strong incentives to meet the privacy concerns and demands of their customers.

But *how* to meet the privacy concerns and demands of consumers when they use the Internet is a much more complex task, and it involves a much larger ecosphere of entities, many of which may not have the same ongoing relationship with – and incentive to protect – consumers' privacy. Moreover, balancing those privacy needs against the uses of consumer information to support legitimate and beneficial Internet services and applications presents new and challenging issues for service providers and policymakers alike.

The Federal Trade Commission's ("Commission") Staff Report, *Protecting Consumer Privacy in an Era of Rapid Change*[2] ("Staff Report") is a commendable effort to address those issues and help meet those challenges. The Staff Report provides a comprehensive analysis of the current state of privacy protection that identifies what appears to be working and what appears not to be working in ensuring that consumers' interests are protected. It proposes a new "framework" for addressing Internet privacy concerns, setting forth its proposed framework as a

[1] This document is substantially similar to the "Introduction and Summary" of comments submitted by the National Cable and Telecommunications Association ("NCTA"), in response to the Federal Trade Commission's Staff Report entitled *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* in February 2011. Though NCTA submitted this paper in its own name, Comcast is an active NCTA member and was a major contributor to this document. The paper accurately reflects Comcast's position, which is echoed by our industry counterparts.

[2] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change*, Staff Report (Dec. 2010), available at http://www.ftc.gov/os/2010/12/101201privacyreport.pdf ("Staff Report").

"policy vehicle," leaving open the question whether the framework might effectively be adopted, in whole or in part, by the affected entities themselves, voluntarily or through self-regulatory mechanisms, or whether it must be mandated by the government.

Regulation in this area must be carefully developed so that it does not constrain the flexibility of Internet entities to tailor their privacy protections to changing technologies, new services, and the evolving economics of the Internet. Regulation – even self-regulation – virtually always produces unintended consequences. And the cost of unintended consequences is uniquely high when they could affect the enormously successful and beneficial Internet ecosystem. Self-regulatory mechanisms are worth exploring and developing in any event, because self-regulation can be quickly modified and adapted to remedy such consequences.

The Staff Report recognizes one of the ways that unduly restrictive or overbroad privacy requirements can have adverse consequences. Specifically, the Commission recognizes the importance of online advertising revenues to the economic underpinnings of Internet content and services. Such revenues supplement, and in many cases substitute for, fees that would otherwise have to be charged to consumers to support such content and services. Without them, the innovation, competition and constant expansion of available content and services that have been the hallmark of the Internet would be impaired. Moreover, forcing more of the Internet's costs to be borne by consumers would undermine the public policy goal of encouraging greater availability and adoption of broadband services. One method of efficiently maximizing the availability of advertising revenues in such a highly competitive marketplace is so-called "targeted advertising" – advertising that is sent specifically to consumers who are most likely to be interested in particular products or services. Targeted advertising may implicate privacy concerns: How do advertisers identify the consumers who are most likely to be interested in their products? The benefits of such advertising must be balanced against such concerns in determining whether and to what extent it should be restricted.

The Staff Report includes many useful ideas and recommendations for balancing the interests at stake in developing a privacy policy framework. A pro-active policy of "privacy by design," for example, minimizes the risk of privacy breaches and concerns from the outset and should be a fundamental component of the development of new Internet products and services by all responsible Internet companies. The cable industry, as noted above, is committed to protecting the privacy of its customers and, to this end, our companies are continually engaged in efforts to develop best practices and promote consumer privacy at every stage of the development of products and services (including the development of targeted advertising policies and procedures).

The concept of "notice and choice" should also play a role in any sound privacy policy insofar as it enables individual consumers to decide, in certain cases, whether the benefits of disclosure of certain consumer information in certain circumstances override any privacy concerns. But the effectiveness of notice and choice can be undermined if it is implemented in a way that is confusing to – or ignored by – consumers. The Commission's proposal to simplify consumer privacy notices by removing from "notice and choice" those transfers of consumer information that are "commonly accepted practices" – or perhaps more appropriately, those for which there is no expectation of privacy – is a step in the right direction.

So, too, is the Commission's recognition that for those practices that remain subject to notice and choice, there may be no single best way to offer such notice and choice in all circumstances. Where disclosure of consumer information can provide benefits to consumers (such as in the case of targeted advertising), notice and choice should be designed to ensure that consumers understand both those benefits *and* the privacy implications. Reflexive opting *out* where a consumer does not fully understand and take into account the *benefits* of disclosure of information is as undesirable as reflexive opting *in* where the consumer does not understand or cannot be expected to take the time to read the details of how and when such information will be disclosed. In particular, a uniform "Do Not Track" button, while providing an easy way to opt out of a privacy-related practice, could lead to just this sort of reflexive and uninformed choice, with unintended and unwanted consequences for consumers. Figuring out how to adapt notice and choice to the vast array of different circumstances in which consumer information may be used and disclosed by Internet content, application, and service providers is precisely the sort of task best implemented through vigilant and ongoing self-regulation.

Caution is warranted before the Commission accepts the suggestion in the Staff Report that the distinction between PII and information that is not personally identifiable has been blurred to the extent that it should no longer be relevant for privacy purposes. Privacy policy (as embodied, for example, in the privacy legislation applicable to cable television operators) has until now generally recognized that the collection and disclosure of aggregate or anonymous data – which can serve wholly legitimate, beneficial, and pro-consumer purposes – does not raise the same concerns or require the same protections as the collection and disclosure of PII. There are also ongoing changes in privacy-enhancing "anonymization" technologies that are designed to *prevent* "re-identification."

Finally, there is a bedrock principle that appears to be missing from the Commission's otherwise comprehensive and commendable Staff Report – the principle of competitive neutrality. In the evolving Internet marketplace, competition extends across the multiplicity of categories of service providers. Cable operators compete, of course, with other broadband Internet Service Providers ("ISPs"), including telephone companies and, increasingly, wireless service providers. But ISPs also compete with other Internet entities – including entities with access to consumer information – in the highly competitive Internet advertising marketplace.

It is crucially important to a fair, efficient and well-functioning marketplace, as well as to the protection of consumers' privacy interests, that any privacy policies apply uniformly to particular *conduct* or types of data collection that affects the privacy interests of consumers and do not single out particular categories of service *providers* for special treatment. In particular, imposing unique or "heightened" restrictions on conduct simply because it is engaged in by broadband ISPs would be especially perverse. As discussed above, ISPs have unique incentives, because of their ongoing relationship with consumers and because of the high cost of losing a broadband customer to a competitor, to be *especially* vigilant in protecting their privacy.