

The agency received a significant amount of input on this issue. Some consumer groups – the Center for Digital Democracy and U.S. PIRG, for instance – urged the Commission to oppose any use of deep packet inspection by network operators. Their view is that the profiling capability of this technology severely threatens consumer privacy.² The Center for Democracy and Technology singled out deep packet inspection because ISPs serve as the gateway to the rest of the Internet and thus have the potential to conduct profound and comprehensive surveillance.³ However, CDT believed that any other technology that could also capture a similarly comprehensive picture of a consumer’s activities should be held to the same standard.⁴

Some industry commenters said that deep packet inspection is not the only technology that can track nearly all of users’ online activity.⁵ For example, we heard from Verizon that cookie based technologies could collect the same – if not more – information than could be captured through deep packet inspection.⁶ The Internet Commerce Coalition argued that if deep packet inspection technology collects the same information as a behavioral advertising network, deep packet inspection should not warrant heightened restrictions.⁷ And the National Cable and Telecommunications Association believed it would be competitively unfair to hold deep packet inspection to a higher standard.⁸

Indeed, numerous technologies can capture large amounts of information about us online or on mobile devices as we go about our lives. Deep packet inspection, social plug-ins, http cookies, web beacons, browser capabilities, a

these distinct profiles experienced the online world in a very different way. Rosen noted that, with comprehensive tracking that will soon be