ATEAC Business Center
Rond Point Schuman 11
B-1040 Brussels, Belgium
Tel. 32.2.888.8462
www.ccianet.org

Computer & Communications Industry Association

October 29, 2010

Via Electronic Mail & Post

La Haute Autorité pour la Diffusion des Oeuvres
et la Protection des droits sur Internet (HADOPI)
4, rue du Texel
75014 Paris, France

Re: Réponse à la consultation publique sur les spécifications fonctionnelles / Response to the Public Consultation on the Draft Functional Specification

Dear Sir or Madam:

On behalf of the Computer & Communications Industry Association (CCIA), I write to express concern regarding the proposed document containing HADOPI's draft functional specification for securing the Internet access of users alleged to have engaged in copyright infringement. CCIA represents large, medium and small companies in the high technology products and services sectors, including computer hardware and software, electronic commerce, telecommunications and Internet products and services – companies with more than $200 billion in annual revenues.

CCIA appreciates France's interest in helping artists and entrepreneurs create, innovate, and make money online. As an association representing Internet commerce platforms, CCIA and its members are keenly aware of how the Internet has created fantastic new opportunities, such as iTunes, Dailymotion, YouTube, and various social media tools, upon which artists may launch careers and reach new markets across the world. The creation of viable marketplace alternatives to infringement has always been and remains a crucial mechanism for protecting both copyright owners and consumers. As we have seen, even as the Internet may challenge certain traditional business models, new technologies are evolving to address these technological challenges. In considering how to help consumers avoid illicit behavior, we encourage HADOPI to not impede these market-driven technological solutions. HADOPI should first do no harm. To this end, while it may be helpful to educate consumers about the options that are voluntarily available to them, technology mandates must be avoided.

In this sense, the draft document suffers from several deficiencies: (a) the invitation to install software under threat of legal penalties hardly creates the appearance of a user option, and this 'invitation' promises to bring various unintended consequences, including encouraging undesirable behavior by repressive governments, which would negatively affect European values

and businesses; (b) it appears to endorse site-blacklisting by third parties other than the software user, *e.g.*, courts; and (c) it stigmatizes neutral Internet protocols, which can impede legitimate uses of Internet technology.

First, any encouragement to install monitoring software under the threat of legal action may appear not to be optional, and may set a precedent that such policies are acceptable. While the proposal is set out as voluntary, it is likely to act as a *de facto* mandate, because users will feel compelled to install specification-complaint applications. Users may perceive that they are presumed guilty of piracy and may have their Internet access terminated unless they "voluntarily" submit to surveillance and logging of their Internet activity. This may also lead users to choose specification-complaint software regardless of its competitive qualifications. In short, the draft specification is likely to have the effect of a technology mandate.

In CCIA's experience, technology mandates are invariably poorly tailored, and have unintended consequences. The technology space is a constantly evolving medium and developing strict guidelines and specifications pertaining to a specific technology (in this case mandating traffic monitoring software with specific guidelines) will prevent the governed software from evolving and adapting as new technologies are introduced. Because applications are constantly evolving, the protocol analysis will not be able to identify them with full accuracy. Thus, the system may drive people to simply shift their behavior from "known" protocols to lesser-known or new ones. Moreover, because it is impossible to determine through protocol analysis whether a given use of the protocol is legal or illegal, the system will invariably be imperfect.

Consumers who want to track their network communications can already use any of a number of general-purpose personal firewall applications that will track port activity. Promoting software designed to government specifications in these circumstances begins down a slippery slope. For example, in module 3, the Specification refers to compiling logs on banned keywords. While an administrator might reasonably want to know when users enter search queries such as "pirate websites," other authorities' interests are focused on different subject matter. The proposed Chinese "Green Dam Youth Escort" software (which was put forth by Chinese authorities to be installed on all Chinese computers in 2009) purported not to police for subversive or anti-democratic content, but rather "unhealthy" and pornographic content. As the reaction to Green Dam indicated,[1] the installation of monitoring software on users' computer, absent any conviction for criminal activity, is not an acceptable policy option, regardless of the ostensible objective.

In any event, the free market has provided end users with a broad selection of effective software applications by which they can secure their Internet connection and protect their computing devices from unwanted communications. There is no need for a governmental authority to prescribe design specifications for software in this properly functioning market, particularly if the intent is to encourage users to install such software while threatening them

[1] Saul Hansell, *U.S. Objects to China Plan to Require Web-Filtering Software*, New York Times, June 24, 2009.

with possible legal sanctions. The imposition of government mandates will only retard market solutions to the problems presented here.

Second, the draft specification refers to blacklists in a manner that might be interpreted to suggest that a software security application's blacklist should be determined by court orders. If an administrator elects to blacklist sites from his or her network hardware, he may do so himself through the use of any number of commercially available firewall applications. Alternatively, the administrator may elect to rely upon a private, commercial security software provider to develop a blacklist. It is inimical to concepts of internet freedom, however, to encourage the installation of software that can restrict users who are not themselves before a judicial authority from accessing a given piece of content. The draft should be amended to clearly reflect that only private sector administrators and users should dictate what content a computing device can access.

Finally, the draft appears to be founded on the misconception that peer-based file transfer protocols are unlawful. The proposed specification must be revised to correct this misunderstanding. While peer-based applications are known to be used for by copyright infringers, numerous legitimate users also employ them. Some developers of peer-based applications have deliberately and willfully encouraged users to infringe copyrights. The actions of a few bad actors should not impugn an entirely communications protocol, however. Like Internet browsers, operating systems, and photocopiers, peer-to-peer software is a neutral apparatus which can be used for lawful purposes, or to infringe copyrights and related rights. BitTorrent, noted in the specification, is used to distribute open source software, popular entertainment content, and in fact powers distributed servers of major social media products such as Facebook and Twitter. The adoption of BitTorrent extends outside of the private sector as well: the British Government's Treasury department, for example, has utilized BitTorrent to distribute large datasets to the public. To discriminate against protocols widely used by the private and public sectors will only impede the lawful distribution of online content.

The proposal also appears to extend beyond peer-to-peer, and may threaten innovation more broadly. The proposal notes the software should check against lists of entities characterized as "black" (prohibited by default), "grey" (may present a risk in terms of counterfeiting and will require user action to override the risk notification), or "white" (authorized entities). Open web platforms – from bulletin boards to video hosting sites, and beyond -- enable a wide swath of legitimate creativity, but are sometimes used for illicit purposes. In such cases, the website owners take the content down after receiving a valid takedown notice. However, if the proposed software would put such sites in the "grey" category, the proposal would deter legitimate use and thus the development of new, legitimate services that can help artists promote their work and make money.

Given that such actions could result in the various unintended consequences noted above, I urge you to reconsider this draft.

Thank you for considering our concerns.

Sincerely,

Erika Mann
Executive Vice President
Computer & Communications Industry Association (CCIA)