



June 29, 2009

Dear Member of Congress:

As the Iranian people are in the midst of a profound struggle for political freedom, social networking sites and Internet messaging services have played major roles in enabling Iranians to coordinate protests, organize rallies, and share political speech. The open Internet's ability to allow people to communicate and organize has allowed Iranians to circumvent the traditional state-run media control in order to challenge the current regime. The use of Internet services such as Facebook, YouTube, and Twitter has been so important for Iranians that Twitter delayed a planned shutdown for maintenance in order to allow this important communication tool to be used without interruption.

Unfortunately, the only thing thwarting Iranians' use of the Internet appears to be the regime's deployment of a relatively new western telecommunications technology called "deep packet inspection," a virtual wiretap which allows the regime to spy on Internet communications and censor their speech. This same technology is used in other repressive regimes to prevent grassroots democratic activism and free expression.

On Monday, June 22<sup>nd</sup>, the Wall Street Journal ran a front page story titled, ["Iran's Web Spying Aided by Western Technology."](#) The story asserts that the Iranian regime, with the cooperation of European telecommunications companies, has installed deep packet inspection technology to monitor Internet communications. According to the story, these Internet control technologies wiretap the Internet connections of private citizens, conduct surveillance on everything end-users do online, and then selectively block, record, or disrupt communications according to the regime's political ends.

Of course, the Iranian government is not disclosing exactly what it is doing to interfere with Internet communications, so it is impossible to know the exact extent to which this technology is being used. We do know, however, that the same technology that aids oppression abroad is currently being deployed here at home by U.S. telephone and cable companies. Network operators are installing deep packet inspection routers throughout their networks in the United States, giving them the same ability to monitor communications of users. They hope to use this controversial technology to inspect Internet communications in order to monetize such communications for advertising purposes or to charge Web sites for preferred treatment on their networks. We do not believe U.S. network owners intend to interfere with political communications in the way the Iranian government is doing, but the control technologies they are deploying on the Internet carry the same enormous power. And, whether an inspection system is used to disrupt political speech or achieve commercial purposes, both require the same level of total surveillance of all communications between end-users on the Internet.



We believe that the unchecked use of deep packet inspection technology has the potential to have a detrimental impact on user privacy and choke off the decentralized, edge-based innovation that has made the Internet the most successful tool for free expression, democracy and innovation ever invented. The situation in Iran highlights the power of technology. We feel it should raise serious questions about how to ensure that deployment of total surveillance, Internet control technologies are restricted exclusively to those instances where the justification outweighs the potential harms.

It has been reported that a bill will be introduced in the Senate that will sanction any company that sells technology aiding the Iranian regime in monitoring or blocking Internet connections or cell phone conversations.

Yet the deployment of deep packet inspection technology is occurring in the United States without full disclosure and government oversight.

We ask that Congress conduct hearings on this issue as soon as possible. The unfortunate situation in Iran provides chilling examples of the dangers of these new technologies. Policymakers must fully understand the implications of wide deployment of deep packet inspection technology so we can make the decisions to prevent its misuse in the United States.

Sincerely,

Open Internet Coalition ([www.openinternetcoalition.org](http://www.openinternetcoalition.org))  
Free Press  
Data Foundry  
Media Access Project  
New America Foundation  
Writers Guild of America, West  
Writers Guild of America, East  
Public Knowledge  
Electronic Retailing Association  
American Civil Liberties Union  
Computer and Communications Industry Association