



**U.S. Department of Justice**

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

May 19, 2008.

The Honorable Howard L. Berman  
Acting Chairman  
Committee on Foreign Affairs  
United States House of Representatives  
Washington, D.C. 20515

Dear Mr. Chairman:

This letter presents the views of the Department of Justice (the "Department") on H.R. 275, the "Global Online Freedom Act of 2008," as reported in the House of Representatives. The Department, of course, shares the general concern motivating the bill – that freedom of expression in the Internet should be protected. Nevertheless, the Department concurs with the views of the Department of State concerning the impact this legislation would have on broader policy issues. Further, the Department foresees the potential to thrust United States businesses into an environment of conflict of laws and to create significant difficulties for the Department in the administration of the bill's requirements, thus seriously compromising the Attorney General's ability to work with foreign law enforcement agencies in an atmosphere of cooperation. Additionally, certain of the bill's provisions raise constitutional questions to the extent they would operate to constrain or jeopardize the President's ability to conduct foreign diplomacy, and to the extent they would operate to regulate the content of U.S. firms' expression in a manner vulnerable to First Amendment challenge.

Moreover, the bill's approach for securing personally identifiable information is one which the United States would likely not countenance if it were applied by foreign entities operating in the United States pursuant to the dictates of foreign law. Consequently, it is the Department's view that the restrictions imposed by the bill may have the unintended effect of prompting foreign countries to preclude United States businesses from operating in their territories, thus having the exact opposite effect of its intended goal, encouraging freedom of expression. Accordingly, the Department opposes the bill as drafted.

The Department's specific comments are set forth below:

**Constitutional Concerns**

Certain of the bill's provisions raise constitutional concerns, specifically foreign affairs and First and Fifth Amendment concerns. Section 101 states that it "shall be the policy of the United States" to promote freedom of speech, to "use all appropriate instruments of United States influence" to advance the cause of free speech, and to deter U.S. companies from cooperating with authoritarian regimes to engage in political censorship. This provision raises

constitutional concerns to the extent it would, particularly when combined with the “global strategy” provisions in section 104(b)(2), operate to constrain or jeopardize the President’s ability to conduct foreign diplomacy with particular foreign countries where other (*e.g.*, national security or economic policy) priorities may require adjustments in the posture that U.S. diplomatic efforts take on intellectual property issues. Sections 205 and 206 raise First Amendment and Due Process concerns, respectively, to the extent that they would (in section 205’s case) compel Internet providers to disseminate information they would not (for policy or legal reasons) otherwise transmit, and (in section 206’s case) purport to give U.S. courts jurisdiction over cases in which a foreign person, while living in a foreign country, provides information from a non-U.S. business to another foreign person to the detriment of yet another foreign party. Finally, the civil penalties established by section 206 could, in some circumstances, raise double jeopardy concerns if used in conjunction with criminal penalties.

### **Sections 2, 3, and Title I generally**

H.R. 275 appears intended to reach efforts to restrict or punish the free availability of information via the Internet, including the prosecution of individuals or groups posting or transmitting “peaceful political, religious or ideological opinion or belief” (*see* Section 103(a)). The bill does not, however, recognize that the “peaceful” expression of political or ideological opinion is a relative term open to interpretation, and that many otherwise-friendly countries routinely prosecute and penalize conduct involving what, in the United States, would be considered protected speech under the First Amendment. Among such countries are Western European nations, in which United States businesses, including those involved in Internet services, have a significant presence. The definition of “Internet-restricting country” may make it difficult to predict which countries would be considered “Internet-restricting,” with the resulting risk that some of these democratic countries would be subject to the restrictions in H.R. 275. Therefore, the bill’s scope may potentially be far broader than the drafters intend.

Furthermore, the definition of “personally identifiable information” (PII) used in H.R. 275 is inconsistent with existing definitions for PII, including those specifically in the OMB memorandum that directs federal agencies in handling such information.

### **Title II generally**

Title II of the bill would forbid United States businesses to locate electronic communications containing personally identifiable information in Internet-restricting countries. It would also prohibit United States businesses from sharing such information with Internet-restricting countries, except for “legitimate foreign law enforcement purposes as determined by the Department of Justice” when the information is transmitted through “established legal channels as determined by the Department of Justice.”

It is possible that these mandates may cause some countries to pass reciprocal laws targeted at the United States. These reciprocal laws may thus restrict United States law enforcement access to similar information located in these other countries’ jurisdiction. Moreover, even without such reciprocal legislation, some countries may restrict the exchange of

law enforcement information that currently is readily available through police or formal judicial assistance channels in response to the restrictions that H.R. 275 would impose. Additionally, this could have the unintended effect of creating “cyberhavens” through which terrorists and other criminals can route their communications, knowing that the data will not be turned over to the United States.

Moreover, we believe it appropriate to raise an issue involving the Electronic Communications Privacy Act (“ECPA”) that illustrates one way in which H.R. 275 may not successfully achieve its goals in preventing disclosure of this information to Internet-restricting countries. Under 18 U.S.C. § 2702(c)(6), providers may disclose customer records, but not content, to “any person other than a governmental entity.” “Governmental entity,” however, is defined in 18 U.S.C. § 2711 to include only U.S. Government entities. Accordingly, ECPA may not protect customer records from disclosure to a foreign government if that foreign government makes the request directly to the provider, rather than through formal legal assistance channels involving the U.S. Government. This separate legal regime raises questions about whether the bill would accomplish its goal.

### **Section 201**

Section 201 would forbid United States businesses to locate electronic communications containing “personally identifiable information” in countries designated as Internet-restricting countries. Because countries are increasingly sensitive to being perceived as “second class” Internet countries, a requirement forbidding United States business from storing information within Internet-restricting countries could lead those countries to take retaliatory steps against United States businesses operating in those countries. Accordingly, section 201 could deter United States businesses from conducting operations in those countries. This effect would be inconsistent with Section 101 of the bill, which would state that United States policy is to promote freedom of expression and the free flow of information. Limiting operations in Internet-restricting countries would decrease the ability of United States businesses to facilitate freedom of expression in those countries.

### **Section 202(a)**

Section 202(a) would prevent a United States business from providing “personally identifiable information ... [concerning an Internet user] to any foreign official of an Internet-restricting country, except for legitimate foreign law enforcement purposes as determined by the Department of Justice.” The Department has several concerns with this provision.

First, the definition of “legitimate foreign law enforcement purpose” would pose problems with respect to implementation. Section 3(8) defines the term as meaning, “for purposes of enforcement, investigation, or prosecution by a foreign official based on a publicly promulgated law of reasonable specificity that proximately relates to the protection or promotion of the health, safety, or morals of the citizens of that jurisdiction,” but the definition excludes “the control, suppression, or punishment of peaceful expression of political or religious, opinion, which is protected by Article 19 of the International Covenant on Civil and Political Rights.” A

foreign government could seek to increase the likelihood that its activities would be considered “legitimate” by stating that it was acting to protect “the health, safety, or morals of ... [its] citizens” and by characterizing the expression as not “peaceful.”

In addition, the definition refers to the “protection or promotion of the health, safety, or morals of the citizens of that jurisdiction.” This language could be construed to exclude situations where an official is seeking information related to a crime committed in another jurisdiction; yet this situation is increasingly common in international investigations that may have to follow an electronic trail through multiple countries. The United States regularly seeks information in this way.

Second, to the extent that the personally identifiable information the bill seeks to protect is located in the United States, it is likely that a foreign government will request such information through formal, legal assistance channels, *i.e.*, pursuant to mutual legal assistance treaties (“MLATs”), letters rogatory, or letters of request. Such assistance requests are directed to the Department, which already determines whether the request complies with legal requirements for its execution, including whether it is made in furtherance of a legitimate foreign criminal investigation, prosecution or proceeding, and rejects requests that implicate constitutionally protected conduct. As noted above, however, if a foreign government makes a request directly to a provider, ECPA may not protect that information from disclosure.

Third, if, in response to the requirements of section 201, a U.S. business locates personally identifiable information in a third country (outside an Internet-restricting country but also outside the United States), the bill’s requirements may place United States law in conflict with the laws and international obligations of that third country. As noted above, some countries not likely to be designated as “Internet-restricting” place limitations on freedom of expression and readily prosecute violators. Such countries may not reject international assistance requests relating to speech-related investigations. For example, if an Internet-restricting country seeks international assistance from the third country by requesting the production of personally identifiable information located in that jurisdiction, the third country may have international obligations to comply with this request, and likely would use its domestic laws to cause the U.S. business to produce the information. In such cases, the third country may conclude that the assistance request from the Internet-restricting country was made for a legitimate law enforcement purpose. Under these circumstances, a contrary determination by the Department would create significant difficulties for the United States and for the United States business, which would be thrust into an atmosphere of conflict of laws. Any attempt by the Department to prevent the U.S. business from producing the information requested would be viewed by the third country as improper. The United States business’ refusal to comply with the third country’s production order may jeopardize that business’ ability to continue to conduct operations in that third country.

### **Section 202(b)**

Section 202(b) would require the Department, after having determined that a request from an Internet-restricting country was “legitimate,” to determine “established legal channels”

for the transmission of information. This language would needlessly require the Department to pass judgment on international law enforcement legal channels and jeopardize the development of new methods of international cooperation.

Moreover, the term “established legal channels” does not appear to be defined in the bill. While conceivably this term could include direct disclosure to a foreign government, we believe it unlikely that the drafters so intend; rather, we believe the drafters intend “established legal channels” to include established legal channels between governmental entities. A requirement that foreign governments seek information only through “established legal channels” used by governmental entities could increase the burden on the MLAT and letter rogatory process, if interpreted to preclude other forms of cooperation, such as assistance through law enforcement channels. The bill could be interpreted to apply this standard not only to the request within the United States, but also to the channels used in the foreign country. Thus, the Department could be asked to opine on whether a foreign law enforcement agency was legally permitted *under foreign law* to seek the information requested - for example, whether the law of country A allows a provincial police department, as opposed to a national agency, to request information about an email customer of a foreign company.

At a minimum, the Department recommends that Section 202(b) be amended to delete “as determined by the Department of Justice.” This amendment would ensure that U.S. businesses use established legal channels used by governmental entities to transmit covered information to foreign officials of countries designated as Internet-restricting countries, while not requiring the Department to pass judgment on which channels are appropriate for the transmission of this information. As noted above, however, this amendment would not address the potential gap under ECPA that may permit foreign governments to directly obtain customer records from providers in the United States.

### **Section 202(c)**

Section 202(c) would create a private right of action for “any individual” aggrieved by a violation of that section. It is unclear how this section would improve freedom of speech and freedom of the press on the Internet. This section would, however, clearly increase the exposure of U.S. businesses to potentially frivolous litigation.

### **Section 206**

Section 206(a) would establish a civil penalty of up to \$2 million for U.S. businesses that violate section 202(a) of the bill and up to \$100,000 for specified individuals acting on behalf of those businesses who violate section 202(a). Additionally, section 206(a) would establish civil penalties of up to \$10,000 for businesses and such specified individuals who violate certain other provisions of the bill. Standing alone, these civil penalties are permissible. If they were used in tandem with a criminal penalty, however, defendants could raise double jeopardy arguments, especially with respect to the higher penalty amounts. Moreover, section 206(a) appears not to permit this civil penalty to be imposed administratively. In contrast, most civil penalty statutes

permit an agency to assess the civil penalty administratively, followed up a civil action if the party involved does not pay the penalty.

Section 206(b) would provide criminal penalties for U.S. businesses and specified individuals acting on behalf of those businesses that willfully violate section 202(a) or certain other provisions of the bill. U.S. businesses that willfully violate section 202(a) would be subject to a fine of up to \$2 million, specified individuals who willfully violate that section would be subject to a fine of up to \$100,000 and five years' imprisonment. U.S. businesses that willfully violate certain other provisions of the bill would be subject to a fine of up to \$10,000, while specified individuals would be subject to a fine of up to \$10,000 and up to one years' imprisonment.

The drafters may wish to consider the relative severity of these punishments, especially as section 206(c) would prevent a U.S. business from paying a civil penalty or fine imposed on a specified individual acting on behalf of that business. Moreover, the provision would also potentially impose criminal penalties on foreign employees of foreign subsidiaries of U.S. businesses. This could include even low-level data handlers, who would be forced to choose between following the law of their own country and U.S. law.

For the reasons explained above, we believe that H.R. 275 is unlikely to promote freedom of expression on the Internet and may, in fact, run counter to that goal by impairing U.S. Government and private sector engagement on this issue worldwide. It also may compromise the Attorney General's ability to work with foreign law enforcement agencies.

Please do not hesitate to contact this office if we may be of additional assistance. The Office of Management and Budget has advised us that from the standpoint of the Administration's program, there is no objection to the submission of this letter.

Sincerely,



Brian A. Benczkowski  
Principal Deputy Assistant Attorney General

cc: The Honorable Ileana Ros-Lehtinen  
Ranking Minority Member