International Trade

April 30, 2012

A New U.S. Sanctions Approach for Syria & Iran – Why Tech and Telecom Companies Are Taking Notice

by Thomas M. deButts, Sanjay J. Mullick & Aaron R. Hutman

The U.S. government would like companies to offer useful technologies and services that enable free communication in Syria and Iran but will also target those who are involved in the direct or indirect provision of goods, services, or technology "likely to be used to facilitate computer or network disruption, monitoring, or tracking that could assist in or enable serious human rights abuses." This challenging balance is the goal of the "GHRAVITY" sanctions introduced by Executive Order effective April 23, 2012. Technology and telecom companies are faced with a number of compliance questions.

The Internet, social networking platforms and new cell-phone media have been a boon to democracy movements and humanitarian causes around the world. This has been captured most vividly in the Arab Spring. The same technologies, however, can be used by governments to monitor, repress and harm their own people. Since technology from a U.S.-based company was found to be filtering Internet access in Syria, the Obama administration has faced difficult questions.

The reaction came on April 22, 2012, with Executive Order 13606, "Blocking the Property and Suspending Entry into the United States of Certain Persons with respect to Grave Human Rights Abuses by the Governments of Iran and Syria via Information Technology" (the "E.O." or "GHRAVITY" sanctions). The E.O. directed the U.S. Treasury's Office of Foreign Assets Control (OFAC) to implement sanctions against one individual and six entities, including a private Syrian telecommunications company (Syriatel) and an Iranian Internet service provider ("ISP") (Datak Telecom). This includes blocking all property and prohibiting transactions with these entities or in circumvention of the E.O.

The E.O. provided standards for identifying new parties that also could be targeted under the order:

- Any person determined by the Secretary of the Treasury, in consultation with or at the recommendation of the Secretary of State:

A. to have operated, or to have directed the operation of, information and communications technology that facilitates computer or network disruption, monitoring, or tracking that could assist in or enable serious human rights abuses by or on behalf of the Government of Iran or the Government of Syria;

B. to have sold, leased, or otherwise provided, ***directly or indirectly***, goods, services, or technology to Iran or Syria ***likely*** to be used to facilitate computer or network disruption, monitoring, or tracking that could assist in or enable serious human rights abuses by or on behalf of the Government of Iran or the Government of Syria; [*emphasis added*]

C. to have materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, the activities described in subsections (a)(ii)(A) and (B) of this section or any person whose property and interests in property are blocked pursuant to this order; or

D. to be owned or controlled by [50% or more], or to have acted or purported to act for or on behalf of, directly or indirectly, any person whose property and interests in property are blocked pursuant to this order.

The E.O. defines information and communications technology as "any hardware, software, or other product or service primarily intended to fulfill or enable the function of information processing and communication by electronic means, including transmission and display, including via the Internet."

The E.O. recognizes the benefits of technology and states that:

> Cognizant of the vital importance of providing technology that enables the Iranian and Syrian people to freely communicate with each other and the outside world, as well as the preservation, to the extent possible, of global telecommunications supply chains for essential products and services to enable the free flow of information, the measures in this order are designed primarily to address the need to prevent entities located in whole or in part in Iran and Syria from facilitating or committing serious human rights abuses.

Implications for Industry

The E.O.'s dual policy goals of fostering communication and preventing suppression confront hardware manufacturers, distributors, software developers, service providers and telecommunications companies with some nuanced compliance challenges to navigate. First, they cannot determine the permissibility of a transaction by relying simply on a reason for control based on an item's classification or characteristics, e.g., that it has low-level encryption. Rather, they must carefully consider, and potentially inquire into, its end use. Second, in examining end use of a product or service, they must consider not only the anticipated or conventional end use, but also other end uses the item potentially may have or facilitate. Companies will now need to consider how third parties may use and pass on their products.

The GHRAVITY sanctions indicate the need for broader and more proactive due diligence considerations, as they apply to the "direct" or "indirect" provision of goods and services "likely" to be used in the listed repressive government activities. For example, companies involved in the emerging field of deep packet inspection ("DPI") will need to be particularly vigilant screening customers and distributors. This may also require extending Know Your Customer ("KYC") procedures beyond the point of initial sale to ongoing requests for service and support. Any knowledge coming into the company that a product with uses

in electronic surveillance, tracking or screening has been diverted to Iran or Syria should consider making a prompt disclosure to the U.S. Government in order to prevent the company itself from becoming a target of sanctions. A company whose software or hardware is traceable, or updates automatically from a home server may face sanctions risks if it has constructive knowledge about a product's use in Iran or Syria. Compliance programs that simply avoid transactional involvement with embargoed countries and U.S.-blacklisted parties may not be sufficient.

The present sanctions are limited to Iran and Syria, where U.S. companies already are restricted from trade, and it is too early to tell whether this approach may be applied to other countries in the future as an anti-repression tool. If the U.S. Government finds evidence of companies located outside of these countries providing services to Iran and Syria, such companies will likely be added to the list. In time, this type of sanctions program could be extended to target repressive regimes in other countries as well. As a result, U.S. and non-U.S. companies may want to consider proactive steps to review countries with which they are doing business and risks for monitoring, repression and human rights abuses.

If you have questions, please contact the Pillsbury attorney with whom you regularly work or the authors:

Thomas M. deButts (bio)
Washington, DC
+1.202.663.8872
debutts@pillsburylaw.com

Sanjay J. Mullick (bio)
Washington, DC
+1.202.663.8786
sanjay.mullick@pillsburylaw.com

Aaron R. Hutman (bio)
Washington, DC
+1.202.663.8341
aaron.hutman@pillsburylaw.com