Written by **Joe Wolverton, II, J.D.** on April 10, 2012

U.S., U.K. Selling Surveillance Equipment to Syria, Iran, and Others

According to a story published by the *Guardian* newspaper in England, an organization called Privacy International has uncovered the sale of high-tech spy equipment from about 30 British firms to the governments of Iran, Syria, and Yemen, among others. The Privacy International report indicates that American and Israeli outfits are also exporting surveillance systems to these nations and others.

The group, the *Guardian* story says, "visited international arms and security fairs" where it was able to verify the sales from at least 30 British firms and 50 firms from around the world, chiefly the U.S., Germany, and Israel.

Included in the planned purchases, the story reports, are the apparatuses necessary to monitor cell phone calls, text messages, and all web activity. There are even devices that will enable the government snoops to hack into citizens' home computers and take remote control of the same.

Frighteningly, statements made by the privacy advocacy organization claim that the surveillance software sold to these countries is so robust that it can give government agents control over the microphones and cameras with which many computers are equipped.

It is little wonder that autocrats around the world are clamoring to get their hands on this technology. They have certainly witnessed with anxious glee the success the sellers have had in deploying the devices in furtherance of their own domestic spying programs.

Information released by Privacy International mentions that among the impressive inventory of advanced monitoring gear being exported from America and the U.K. is something called an IMSI (International Mobile Subscriber Identity) catcher.

Surveillance experts informed *The New American* that an IMSI catcher basically functions as a false cellular relay that intercepts signals sent back and forth between a cell phone and a provider's legitimate tower.

If used by those with proper training, the IMSI catcher will be invisible to the cell phone user and to the cell phone company and it will provide the person maliciously deploying the device with tracking data that is sent from the phone — data intended for use by the towers and switches owned by the cell phone company.

Curiously, in a decision handed down earlier this year, the Court of Appeal of England and Wales denied the issuing of a patent for the device. Conveniently, prohibiting a patent on the IMSI catcher facilitates the government's own sale of them to the highest bidder without regard for a manufacturer's interest.

Privacy International claims that the United States and Britain have bundled malware with the IMSI catchers. Malware is software that once installed on a target's computer can give the installer absolute control over all the systems and devices attached to that computer, leaving the perpetrator undetected.

Perhaps the most chilling aspect of this story is the sale by the U.S. and England of something called "optical cyber solutions," described in the *Guardian* piece as something that "can tap submarine cable landing stations, allowing for the mass surveillance of entire populations.... "

If the information provided by Privacy International is accurate, then again, it is easy to recognize something in common between the buyers and the sellers. The group declares, "The emerging information and communications infrastructures of developing countries are being hijacked for surveillance purposes, and the information thereby collected is facilitating unlawful interrogation practices, torture and extrajudicial executions."

Sadly, there is nothing more American in the post-Patriot Act world than unlawful interrogations, torture, and extrajudicial executions. Birds of a feather flocking together, it would seem.

There is evidence of the shocking accusations made by Privacy International against the governments of the United States and the United Kingdom. Examples of several collateral promotional items (brochures, videos, etc.) put together by the manufacturers of the goods being offered for sale by representatives of these companies have been posted on the Internet by WikiLeaks.

Additional evidence was published recently by the *Wall Street Journal*. In a story from November, 2011, the rapid expansion of the surveillance marketplace was described:

> The techniques described in the trove of 200-plus marketing documents, spanning 36 companies, include hacking tools that enable governments to break into people's computers and cellphones, and "massive intercept" gear that can gather all Internet communications in a country. The papers were obtained from attendees of a secretive surveillance conference held near Washington, D.C., last month.
>
> Intelligence agencies in the U.S. and abroad have long conducted their own surveillance. But in recent years, a retail market for surveillance tools has sprung up from "nearly zero" in 2001 to about $5 billion a year, said Jerry Lucas, president of TeleStrategies Inc., the show's operator.

Officially, of course, the United States, the United Kingdom, and the European Union are ardently opposed to any such sale of surveillance technology to the identified regimes.

On March 23 of this year, for example, the Council of the European Union enacted Council Regulation No. 267/2012, which proscribes the "exports of equipment and software intended for use in the monitoring or interception of internet and telephone communications by the Iranian authorities." Similar bans are already in place to govern the sale of such goods to Syria.

For its part, the United States has imposed similar bans on sales to Syria and other "enemies." In another article published in the *Wall Street Journal* by the same investigative reporter, however, the porousness of these barriers is revealed:

> A U.S. company that makes Internet-blocking gear acknowledges that Syria has been using at least 13 of its devices to censor Web activity there — an admission that comes as the Syrian government cracks down on its citizens and silences their online activities.
>
> Blue Coat Systems Inc. of Sunnyvale, Calif., says it shipped the Internet "filtering" devices to Dubai late last year, believing they were destined for a department of the Iraqi government.

> However, the devices — which can block websites or record when people visit them — made their way to Syria, a country subject to strict U.S. trade embargoes.

The leadership of Privacy International anticipates that such sanctions will continue to serve as mere sieves through which critical technology will continue to flow into the wrong hands, and they are too little, too late.

"By the time the embargo is in place the ship has sailed," said Eric King, head of research at Privacy International.

The article in the *Guardian* lists several British and European companies that are suspected of supplying surveillance equipment to Egypt, Iran, and Syria in defiance of active embargoes.

Given the scope of the problem, the human rights abuses perpetrated by the buyers (and too often, the sellers), and the participation of American and British concerns in the condemned commerce, it is worth staying abreast of the situation and the growth of the industry.

It is likely that as citizens of the free nations of the world successfully push back against the secret policy of their leaders to install surreptitious, round-the-clock monitoring of their every movement, the men and women living under less liberal governments will take heart and redouble their efforts to blind the unblinking eye of Big Brother that watches them, as well.