Strictly Confidential

By Jacob Shapiro

July/August 2007

Why professors and analysts are our best secret weapon.

Everyone says an open, transparent government is the hallmark of a healthy democracy. But most reasonable people would agree that there must be limits to how transparent government can be. After all, no one wants sensitive national security secrets to fall into the wrong hands. When information shared in the name of good governance can be exploited by terrorists, many would argue the public’s right to know pales in comparison to the public’s need for protection.

But are openness and security really opposing values? When government officials curb access to information, they cut themselves off from the brain power and analytical skills of a huge community of scientists, engineers, and security experts who are often far better at identifying threats, weaknesses, and solutions than any government agency. The effort to cordon off experts from sensitive information has been dramatic, especially in the United States. An executive order signed by President George W. Bush in 2003 permitted—some say encouraged—the U.S. government to classify mountains of information. For the first time, basic infrastructure information was designated as a category of classifiable information. The increase in secrecy has been staggering: In 1996, 5.8 million documents were classified by the U.S. government. In 2005, that figure nearly tripled, to 14.2 million documents stamped “secret” or “confidential.” Even
more information has been kept from the public by an increase in
the use of “sensitive but unclassified” markings, which operate without the legal constraints of the traditional
classification system. In 2006 alone, just the number of categories under which a document might be labeled
“sensitive” increased by 20 percent. But this added secrecy hasn’t made anyone safer. In truth, it is leaving everyone
more vulnerable to emerging threats.

Consider the efforts of Lawrence Wein, a Stanford University business professor, and his then graduate student,
Manas Baveja. In research published in 2005, Wein and Baveja analyzed the effectiveness of the U.S. Visitor and
Immigrant Status Indicator Technology, a fingerprint identification program designed to prevent known terrorists
from entering the United States. Using information on fingerprint readers from the Web site of the National Institute
of Standards and Technology (NIST), the federal agency that tracks the United States’ technology infrastructure, they
found that terrorists could take advantage of the system by reducing the image quality of their fingerprints. (Simply
rubbing one’s fingers with sandpaper would do the trick.) They also found an easy solution: Require people to
present more fingers if their prints were poor. The fix made the program more effective even though terrorists knew
exactly how the system worked. Immigration officials quickly adopted a version of Wein and Baveja’s idea. But NIST
responded by removing the information Wein and Baveja used for their analysis from its Web site.

Or, take graduate student Sean Gorman’s 2003 dissertation at George Mason University. Gorman used public
information to map the fiber-optic network of the United States, identifying critical choke points in the country’s
telecommunications infrastructure. Under pressure from government officials, Gorman ultimately agreed to redact
many of his most sensitive findings. Today, parts of his research remain classified, and much of the information
Gorman used is no longer publicly available. But this reaction misses what was so valuable about his study. In
identifying dangerous vulnerabilities, Gorman found efficient ways to remove them. Putting information behind lock
and key does not make targets safe from attack. It leaves security analysts unable to find solutions to other
weaknesses in the future. It also leaves government and industry less motivated to find safeguards of their own.

Harvard University’s Efraim Benmelech and the RAND Corp.’s Claude Berrebi took up research on a project with
unmistakable relevance to everyone’s national security. Using publicly available data from the Israeli Security
Agency, they found that not only are older, better-educated suicide bombers assigned to more important targets but
that these bombers are deadlier in their attacks. Their analysis depended critically on having access to data about
failed attacks, information that most other governments restrict out of fear that it can prove useful to terrorists. But
understanding how terrorist groups assign operatives to missions does more to combat terrorism than the Israeli
government’s openness did to abet it.

Governments must do a better job of assessing when the benefits to sharing information will exceed the costs. The
question should not be, “Can this information help terrorists at all?” It should be, “Will sharing this information do
more to protect society than it will to help those who wish us harm?” In determining the trade-offs, common sense is
the most natural guide. When governments don’t fully understand a system’s vulnerabilities, information should be
shared so that analysts can find solutions before terrorists identify weaknesses. Similarly, information about known
vulnerabilities should be shared when terrorists can easily identify the target.

The thinking capacity of a huge network of universities and research centers should be considered a national security
strength, not a threat or nuisance that needs to be kept at arm’s length. The academy’s powers to analyze dangers
and recommend safe, efficient solutions are stronger than that of the government, and infinitely stronger than that of
any terrorist organization. When governments consider everyone a potential terrorist, they are insulating themselves
from the brain power that should be our first line of defense.

Jacob Shapiro is a predoctoral fellow at Stanford University’s Center for International Security and Cooperation.