Backgrounder

Published by The Heritage Foundation

No. 1810
November 5, 2004

Protecting Privacy and Providing Security: A Case of Sensible Outsourcing

James Jay Carafano, Ph.D., and Paul Rosenzweig

Defending the nation against terrorists, promoting economic growth, and protecting constitutional liberties are all prerequisites for a sound homeland security strategy. At one time or another, outsourcing[1] has been labeled a threat to all three. These criticisms are simply overblown. In fact, if the U.S. partners with nations that share a commitment to the rule of law, transparency, and open competition, it can use sensible outsourcing to enhance the protection of the privacy of American citizens, promote better security practices, and contribute to economic prosperity. Effective outsourcing can provide both cost-effective services and appropriate protections for government and commercial activities supported by overseas vendors.

India is an example of an increasingly important strategic ally that has begun to develop the right capacities in its business process outsourcing (BPO) industry to be a good global economic and security partner. Administration policy should encourage closer cooperation on security issues and encourage India to expand its market reforms of the BPO industry to other economic sectors. Meanwhile, congressional legislation should encourage, not impede, the ability of the government and the private sector to get the best, most reliable and secure technology and services for the best price. Finally, the U.S.–India relationship should become a model for expanding economic and security cooperation between developed and developing nations.

Talking Points

- The United States can use sensible outsourcing to enhance the protection of the privacy of American citizens, promote better security practices, and contribute to economic prosperity.
- Market forces can help to enhance both economic growth and security.
- The federal government and the Department of Homeland Security can and should award contracts to the companies that will provide them with the best security for value paid, regardless of where the work will be done.
- Congressional legislation should encourage, not impede, the ability of the government and the private sector to get the best, most reliable and secure technology and services for the best price.

This paper, in its entirety, can be found at:
www.heritage.org/research/homelanddefense/bg1810.cfm

Produced by the Kathryn and Shelby Cullom Davis
Institute for International Studies

Published by The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002–4999
(202) 546-4400 • heritage.org

Nothing written here is to be construed as necessarily reflecting the views of The Heritage Foundation or as an attempt to aid or hinder the passage of any bill before Congress.

Outsourcing and Security of Data and Services

The question of outsourcing and security received considerable public attention after the Department of Homeland Security (DHS) awarded a contract for US-VISIT (a project designed to monitor the entries and exits of non-U.S. citizens) to Accenture LLP, a U.S. subsidiary of a Bermuda-based corporation. Among the concerns raised was that data and processes managed by an overseas company might pose greater security risks. In a previous research paper, Heritage Foundation analysts argued that concern was simply unwarranted.[2] Outsourcing does not automatically increase the vulnerability of the United States, nor is outsourcing an economic threat.

The federal government and the Department of Homeland Security can and should award contracts to the companies that will provide them with the best security for value paid, regardless of where the work will be done. Protectionist policies only stifle innovation and increase costs. "Where the contract is fulfilled—whether in Boston, Britain, or Bermuda—does not necessarily add to or detract from the end goal of protecting America."[3] Processing the data in the United States does not guarantee that the information will be safe. The proper way to protect privacy and to enhance security for both government and private sector programs is through stringent service and data protection requirements; choosing only companies that can satisfy all of these requirements while also expertly completing projects; and selecting companies with good management that operate in countries with strong rule of law. In short, both the public and private sectors can achieve the appropriate levels of privacy protection and reliability of service if they insist that contract work is conducted in countries that have a cooperative relationship with the United States across a broad spectrum of trade security initiatives.

It is particularly important that the U.S. government insist upon stringent security standards when dealing with sensitive or confidential information, whether the data regard national security concerns or the privacy of individual citizens. Physical security, data protection systems, robust law enforcement forensic capacity, audit and trace access to information systems, and strong legal protection are all important parts of that security. Any contract award that does not provide for these types of measures could compromise U.S. security, regardless of which company is awarded the contract or where the work will be done. On the other hand, engaging in mutually beneficial cooperative business ventures with companies in countries that meet appropriate criteria is simply sensible outsourcing.

India as a "Trusted Provider"

India's potential as a global security and economic partner illustrates the potential and the challenges of intelligent outsourcing. Indian companies could potentially provide a variety of useful technologies and services. As one industry observer concluded:

> The Indian BPO [business process outsourcing] industry has grown at a mind-boggling 60–70 percent annually, with revenues rising from US$565 million in 1999–2000 to almost $2.4 billion in 2002–2003. The projections look brighter too—employment of over a million people by 2006, up from the current 200,000. Revenues are estimated to increase to well over the current $2.4 billion mark by 2006.[4]

[1] Outsourcing is the transfer of a business process, such as customer service or the development of computer software, to an overseas provider.

[2] For more information, see James Jay Carafano, Tim Kane, Dan Mitchell, and Ha Nguyen, "Protectionism Compromises America's Homeland Security," Heritage Foundation *Backgrounder* No. 1777, July 9, 2004, at *www.heritage.org/Research/HomelandDefense/bg1777.cfm*.

[3] *Ibid.*

[4] Siddharth Srivastava, "If Only Indians Would Talk Like Americans," *Asia Times*, January 8, 2004, at *www.atimes.com/atimes/South_Asia/FA08Df04.html* (September 22, 2004).

As Indian firms gain both greater expertise and market share in the BPO sector, they will have increasing capacity to meet the full range of U.S. service needs for both the government and the private sector.

India's emerging approach to information security and critical infrastructure protection demonstrates how market forces can help to enhance both economic growth and security. As the market share devoted to offshore work has increased, data security has become a key focus of Indian information technology (IT) companies.

> Information security can be broadly classified under network security (security of storage and transmission infrastructure), physical security (security of work areas, documents), personnel security (security against threat from employees), and business continuity and disaster recovery (contingency plans to retrieve information and prevent loss in the case of emergencies).[5]

Indian companies are increasingly providing all of these.

Because of concerns of companies and governments that are considering outsourcing, Indian businesses are under great pressure to adopt best practices and provide security environments equivalent to that of their competitors. As a result,

> Measures taken by companies include complying with international security standards, establishing security policies, making provisions for security spending in the IT budget, among others. Larger companies have dedicated teams responsible for ensuring security, employ latest technologies, conduct security training and awareness programs, and form specific policies for personnel and physical security.[6]

Indian companies tend to allocate between 5 percent and 15 percent of their budgets for security.[7]

Indian network security involves basic technologies like antivirus and firewall software. In addition, if client requirements warrant them, advanced technologies such as intrusion detection systems, encryption, authentication, and access controls are used. Physical security at many Indian companies includes multiple-level physical access control systems, 24-hour security guards, and clear desk and clear screen policies.[8] Because most companies believe attacks are generated internally, personnel security involves a three-pronged approach: employee screening with background checks, training, and a robust disciplinary process. In addition, some Indian companies also have continuity and disaster recovery plans. Many industry members also have efficient security mechanisms and policies in place.

> Most leading companies have very robust security practices. However, smaller companies have the basic technologies and policies in place, but are constrained by return on investment as far as investing in security is concerned.[9]

In addition to private sector initiatives to become a trusted outsourcing center by using best practices and international security protocols, the Indian legislature is also attempting to make the country more attractive to potential clients. In 2000, the legislature passed the Information Technology Act of 2000, which "covers only unautho-

[5] Evalueserve, "Information Security—Indian Offshore Service Providers," National Association of Software and Service Companies (India), 2002, at *www.nasscom.org/artdisplay.asp?Art_id=3087* (October 26, 2004).

[6] *Ibid.*

[7] *Ibid.*

[8] A clear desk policy requires sensitive information to be locked up when the work area is unattended. A clear screen policy mandates that workstations or other information systems lock themselves after a certain period of time and require an authorized user to sign on before it can be used again. These policies are consistent with the requirements of ISO 17799. For more information, see CITSEC, "Guidance for Completion of an ISO17799-Compliant Security Regime," at *www.citsec.com/it-security-ISO-17799-guidance.htm* (September 24, 2004).

[9] Evalueserve, "Information Security."

rized access and data theft from computers and networks, with a maximum penalty of about $220,000, and does not have specific provisions relating to privacy of data."[10] This fall, it is expected to take up legislation amending the 2000 Information Technology Act. The amendments will likely conform to the adequacy norms of the European Union's Data Protection Directive[11] as well as U.S. Safe Harbor[12] privacy principles.

The EU Data Protection Directive prevents the transfer of personal data to non-EU nations that have not been certified as having adequate privacy protections. This directive relies on comprehensive legislation that requires, for instance, the establishment of government data protection agencies and registration of databases with those agencies. Because the United States takes a more segmented approach to privacy protection—relying on a mix of legislation, regulation, and self-policing—it had to develop a means for U.S. companies to comply with the EU directive. U.S. companies that use this Safe Harbor program are not hampered in their European operations. The program, which was approved by the EU in 2000, allows U.S. companies that enroll in the program to avoid delay in business dealings and prosecution under EU privacy laws. The companies are deemed to meet EU privacy standards.[13] If the Indian legislative changes meet the EU standards, India will become an even more significant source of data processing, as information about citizens of the EU countries can then be processed in India.

In addition, the National Association of Software and Service Companies (NASSCOM), a major representative of software and service companies in India, has been advocating that Indian regulations should also meet U.S. industry specific requirements (e.g., the Health Insurance Portability and Accountability Act) as well as state laws. To improve the perception of security and the willingness to prosecute computer crimes, NASSCOM has also helped to establish designated cybercrime sections within police departments in which specially trained investigators focus solely on computer crimes.

In the absence of a stronger protections regime, foreign outsourcing customers have had to incorporate their privacy and data security requirements into a legally binding contract with Indian vendors. Contracts with U.S. outsourcers frequently specify New York as the controlling jurisdiction and require insurance, which is usually provided by a U.S. carrier. Contract remedies for breaches may be problematic, however, because determining an appropriate remedy or damage amount is frequently difficult.

The Next Steps

India's current laws regarding electronic commerce, copyright and patent protection, identity theft, privacy, and cyberterrorism must be strengthened. Revising the Information Technology Act of 2000 must be a priority, but more also needs to be done.

[10] John Ribeiro, "Indian Law May Satisfy Data Protection Concerns," *Computerworld*, April 21, 2004, at *www.computerworld.com/databasetopics/data/story/0,10801,92557,00.html* (October 26, 2004).

[11] For the text of the law, see *Official Journal of the European Communities*, No. L. 281, November 23, 1995, p. 31. An unofficial text of the law is available at *www.cdt.org/privacy/eudirective/EU_Directive_.html#HD_NM_0* (October 26, 2004).

[12] For more information, see U.S. Department of Commerce, "Safe Harbor Overview," at *www.export.gov/safeharbor/sh_overview.html* (September 24, 2004).

[13] Safe Harbor principles require: (1) notice of purposes for which information is collected; (2) choice to opt out of having information disclosed to a third party; (3) transfer to third parties as agents may only be done if the agent subscribes to Safe Harbor principles, the EU directive, or another adequacy certification; (4) access to personal information held about the person so that she or he can change, correct, or delete inaccurate information; (5) reasonable security cautions to protect information from loss, misuse, unauthorized access, disclosure, or alteration; and (6) data integrity (information must be reliable for its intended purpose). At least one U.S. privacy organization has argued that the Safe Harbor program allows for preferential treatment of EU information and for "second-class" privacy protections for U.S. citizens' information. See Deirdre K. Mulligan, letter to the Honorable David L. Aaron, December 3, 1999, at *www.ita.doc.gov/td/ecom/cd&t1299.htm* (September 24, 2004).

As promising as the growth of the Indian BPO sector and the effort of IT companies to perform due diligence in protecting information and ensuring continuity of service has been, more needs to be done for India to fulfill its potential as a global economic and security partner. According to the *Financial Times*, direct foreign investment in India is "anaemic,"—$4 billion compared to $50 billion for China.[14] The lack of foreign investment has hamstrung India's efforts to expand and update its infrastructure, modernization that is critical to spurring further economic expansion. In large part, the lack of investment reflects the absence of reform in the Indian economy outside the IT sector. According to the *2004 Index of Economic Freedom*, "the government continues to restrict 700 sectors to small-scale industries, preventing larger companies from taking advantage of economies of scale."[15] Trade barriers and excessive regulation discourage overseas private investment. Additionally, artificial barriers that keep U.S. goods and services out of Indian markets have slowed the growth of robust U.S.–Indian partnerships. India should adopt reforms to reduce government regulations and liberalize its protectionist trade polices to encourage more foreign investments. A wave of bold reforms on the part of India would do much to strengthen U.S.–Indian economic ties, undercut unwarranted criticisms about outsourcing, and reduce concerns about potential security risks from BPO activities.

In turn, the United States should put in place the right framework to take full advantage of opportunities offered by Indian BPO companies. In particular, Congress should facilitate a predictable business environment that will ensure that overseas companies will not be unfairly discriminated against based on unwarranted security concerns. For example, Congress should remove Section 835 "Prohibition on Contracts with Corporate Expatriates" from the Homeland Security Act.[16] DHS should have the power to award contracts to any company that can perform services effectively, efficiently, and securely. Meanwhile, DHS and other federal agencies that may wish to outsource homeland security work overseas should establish programs similar to the Department of Defense's National Industrial Security Program, in order to provide BPO companies with clear guidance about the requirements and standards for performing security-related services.[17]

What the U.S. Government Should Do

India's efforts to become a "trusted provider" of IT services are laudable. They have established the foundation for mutually beneficial economic and security partnership, one that could serve as a model for U.S. cooperation with other developing nations. More must be done, however, to fully exploit the potential of U.S.–Indian cooperation. While India should continue its efforts to create a strong privacy regime for all information being processed within the country, the U.S. government should:

- Consider outsourcing data processing where possible, but also be careful to choose companies (and countries) that will provide the most security value for the money spent;
- Outsource data processing where appropriate, but ensure that the BPO vendor and the country meet stringent privacy standards; and
- Eliminate regulatory barriers that impose unwarranted prohibitions against outsourcing.

[14] Khozem Merchant, "Indian Credit Quality at a 10-Year High," *Financial Times*, October 7, 2004, p. 20.

[15] Marc A. Miles, Edwin J. Feulner, and Mary Anastasia O'Grady, *2004 Index of Economic Freedom* (Washington, D.C.: The Heritage Foundation and Dow Jones & Company, Inc., 2004), p. 219, at *www.heritage.org/index*.

[16] Homeland Security Act of 2002, Public Law 107–296. As it stands, §835(a) states that "The Secretary may not enter into any contract with a foreign incorporated entity which is treated as an inverted domestic corporation." Subsection (d) of §835 entitled "Waivers," however, gives the Secretary of Homeland Security the right to waive Subsection (a) in the interest of homeland security, to prevent the loss of any jobs in the U.S., or to prevent the government from incurring any additional costs. This substantially limits the prohibitions set by §835.

[17] Carafano *et al.*, "Protectionism Compromises America's Homeland Security."

Conclusion

The goal of increasing domestic security and protecting the privacy of U.S. citizens should not be an obstacle to strengthening economic ties with the developing world. Rather, market forces and sensible outsourcing can be used both to promote better global security practices and to encourage economic growth.

—James Jay Carafano, Ph.D., is Senior Research Fellow for National Security and Homeland Security in the Kathryn and Shelby Cullom Davis Institute for International Studies at The Heritage Foundation. Paul Rosenzweig is Senior Legal Research Fellow in the Center for Legal and Judicial Studies at The Heritage Foundation and Adjunct Professor of Law at George Mason University. Alane Kochems, a research assistant at The Heritage Foundation, contributed to this paper.