Outsource Your IP Legal Work at Your Client's—and Your—Peril

By Joseph A. Hennessey

Pundits speak as if international borders are increasingly irrelevant in the modern world. Thomas Friedman, in his much-acclaimed book, *The World Is Flat*, has stated: "Globalization . . . is shrinking the world from a size small to a size tiny and flattening the playing field at the same time. . . . [T]he thing that gives it its unique character is the newfound power for individuals to collaborate and compete globally."[1]

No doubt, the digitization of commerce has transformed every level of industrial activity, including engineering, original equipment manufacturing and supply-chain management. Globalization promises new levels of efficiency in service industries as well. Customer service call centers, help-lines, and credit card operations have been outsourced to low-cost providers for years. Outsourcing is moving up the food chain as digitization in the accounting, financial, insurance, and healthcare sectors facilitates offshore provision of those services. Naturally, one would guess, legal services can and should follow the lead of other digitized professions in order to meet quality and price demands of clients . . . right?

Not so fast. The world is not flat with respect to the provision of legal services. Even a cursory review of U.S. Supreme Court precedent reveals that the judicial branch views legal rights and processes as specially protected within the United States' territorial possessions.[2] U.S.-based attorneys and their

Joseph A. Hennessey is a complex litigation partner with Beins Goldberg & Hennessey, LLP, in Chevy Chase, Maryland. He specializes in complex business litigation and arbitration. He can be reached at jhennessey@bghllp.com.

clients enjoy more rights under the United States Constitution than foreign-based counterparts.[3] Those who yield this comparative advantage by outsourcing client legal services to foreign nationals who reside overseas do so at their client's—and their own—peril.

Economic Warfare on the Digital Frontier

There are relentless efforts to encourage U.S. attorneys to outsource the provision of legal services to low-cost foreign attorneys operating overseas (referred to generically as "legal process outsourcers" or "LPOs").[4] The impulse to jump on the outsourcing bandwagon comes at the expense of a critical analysis of the threats posed to our clients by moving their information and their legal work outside the protections of U.S. laws. U.S. attorneys should be wary of using foreign nationals to process legal work, not because such wariness placates xenophobic prejudices, but because U.S.-based attorneys are better protected against a variety of governmental intrusions and other threats than are foreign-based attorneys. Legal process outsourcing poses particular threats to attorneys working to protect intellectual property. Not only does outsourcing legal services place our clients in environments with relatively diminished legal protection, it inserts them into virtual economic warfare waged to capture gem trade secrets and innovations.

The opening of the digital frontier has undeniably and exponentially expanded the combat zone in which nations compete for economic advantage. According to the FBI, at least 23 foreign governments, including France, Israel, Russia, China, Iran, Cuba, the Netherlands, Belgium, Germany, Japan, Canada, and India, actively target the intellectual property of U.S. corporations.[5] The most frequently targeted industries appear to include aerospace, biotechnology, computer software and hardware, transportation and engine technology, defense technology, telecommunications, energy research, advanced materials and codings, stealth technologies, lasers, manufacturing processes, and semiconductors.[6]

As more and more of our economy is digitized, it becomes more vulnerable to government-sponsored espionage and theft. In days past, intelligence gatherers relied on surreptitious entry and the theft of information reduced to printed media. Such physical limitations are increasingly absent in today's business environment. As has been explained,

> [p]rior to the employment of digital memory devices and network connectivity, intelligence operatives were limited with respect to the scale of their operations and individual case officer and agent supervisory spans of control. "Cyber case officers" using virtual agents do not have the scale of their operations limited to a finite number of "cyber agents" but, instead, can deploy virtual cyber resources in unlimited quantities simultaneously. These cyber agents can respond to multiple collection requirements, remotely targeting multiple objectives simultaneously with limited risk. The reduction in risk is due to the absence of physical constraints present in traditional intelligence operations.[7]

The impact of sustained economic warfare against intellectual property assets has been devastating. The American Society of Industrial Security, U.S. Chamber of Commerce, and PricewaterhouseCoopers have utilized a 2002 survey of Fortune 1000 corporations and 600 small- to-midsized U.S. companies to estimate that proprietary information and intellectual property losses due to economic espionage amount to approximately $53 billion to $59 billion.[8]

Inadequate Law Enforcement Abroad

The threat posed by government-sponsored economic espionage is compounded by private theft of intellectual property and the flat-footed response by some overseas law enforcers. The experience of U.S.-based Jolly Technologies has bubbled to the surface in the discussion of outsourcing risk. According to published reports, California-based Jolly Technologies reported the theft of portions of its source code and confidential design documents relating to one of its key products at its new research and development center in Mumbai, India. Jolly Technologies claimed that its efforts to pursue the matter were met with "utter and total reluctance to get involved" by the Mumbai police department.[9] According to these same published reports, Jolly Technologies alleged that top law enforcers in Mumbai claimed to be unaware of any intellectual property protection laws and refused to acknowledge the complaint. "In an era where American corporations are outsourcing more sensitive data than ever before," said a Jolly Technologies spokesperson, "Indian authorities appear ill-prepared and extremely reluctant to handle the law enforcement duties required to support such an environment."[10] The acrimonious exchanges between Jolly Technologies and Mumbai law enforcers have drawn comment from those covering outsourcing and intellectual property matters.

> The allegations and counter-allegations highlight long-standing problems. Indian laws do provide protection against IP theft but enforcing them is a huge challenge. Law enforcement agencies lack awareness about cyber crimes, while more often than not, officials are not trained to tackle them.[11]

USPTO Response

The threat that legal outsourcing poses to secrets has not been lost on the United States Patent and Trademark Office. On July 23, 2008, the USPTO published a short yet revealing statement of policy in the *Federal Register*. Responding to the fact that "a number of law firms or service provider companies located in foreign countries are sending solicitations to U.S.-registered patent practitioners to offer their services in connection with the preparation of patent applications to be filed in the United States," the USPTO made clear that attorneys can *only* transmit data and materials for the preparation of patent applications that they are already authorized to export under the Export Administration Regulations (EAR) of the Department of Commerce's Bureau of Industry and Security. Specifically, "if the invention was made in the United States, technical data in the form of a patent application, or in any form, can only be exported for purposes related to the preparation filing or possible filing and prosecution of a *foreign* patent application, after compliance with the EAR or following the appropriate USPTO *foreign* license procedure."[12] In addition, the USPTO has made clear that "[a] foreign filing license from the USPTO does not authorize the exporting of subject matter abroad for the preparation of patent applications to be filed in the United States," as export for such purposes is not covered by the terms of the USPTO's foreign license.[13]

From the NSA to the FBI or SEC

While concerns about foreign economic espionage should trouble IP attorneys, the eavesdropping and intelligence-gathering capabilities of the U. S. Government should give IP attorneys—and all members of the bar—additional pause. The simple truth is that no government has greater capability to harvest private and public secrets than the U. S. government. Not long ago, the federal government refused to acknowledge the existence of the National Security Agency (NSA). Now revelations about monitoring of communications by the NSA have produced chilling information about the extent to which the NSA harvests international communications to meet its charge of gathering national security intelligence.

When a U.S.-based attorney places a call within the United States, that attorney has a reasonable expectation of privacy in the call. This expectation of privacy is protected by the Fourth Amendment and bolstered by statute enacted by Congress through 18 U.S.C. § 2511(1)(a). However, the moment a U.S.-based attorney dials a foreign national who resides overseas, Fourth Amendment and statutory expectations of privacy are nullified.[14] When a U.S.-based attorney accesses the international telephone system by dialing "011," or when a U.S.-based attorney clicks "send" on an electronic transmission destined for a foreign terminus, that attorney's communications have left the United States and its constitutional and statutory protections.

According to reports published in legal periodicals, the NSA intercepts international telecommunications through an eavesdropping network known as ECHELON.[15] ECHELON is an automated global satellite-based interception and relay system operated by the intelligence agencies of five nations: the United States, Britain, New Zealand, Australia, and Canada. It has been estimated that ECHELON intercepts as many as 3 billion communications every day, including phone calls, email messages, Internet downloads, and satellite transmissions. The memory buffers maintained by NSA are thought to be capable of storing five trillion pages of data.[16] Raw data from ECHELON intercepts are relayed to NSA memory buffers where they are digitally searched using key words and phrases supplied by the intelligence agencies of the five participating countries.[17] Information seized by NSA can be freely transferred to any agency in the federal government. This explicit legal authority has existed for 26 years—ever since the Sixth Circuit Court of Appeals handed down its opinion in *Jabara v. Webster* and the Supreme Court denied certiorari in 1983.[18] In that case, Abdeen M. Jabara, described by the Sixth Circuit as "a Detroit lawyer of Arab extraction," had been the subject of both FBI and NSA surveillance. The court explained, "On November 1, 1971, the FBI, without a warrant, requested the NSA to supply it with the contents of Jabara's telegraphic communications sent overseas, and the NSA complied by furnishing the FBI with summaries of six of such communications."[19] Jabara did not challenge the legality of NSA's interception of his communications; instead he claimed that "his rights were violated when the NSA turned over the information, without a warrant, to the FBI."[20]

In deciding this point, the Sixth Circuit pointed out that "Jabara's very words, summaries of which were supplied to the FBI, had been lawfully intercepted by and were in the records of the NSA. NSA therefore already had in its records, after it intercepted, all that it supplied to the FBI."[21] While acknowledging that attorney Jabara might have had a subjective expectation of privacy with respect to his international calls or even a subjective expectation that intercepts made for intelligence-gathering purposes would be husbanded within NSA, the Sixth Circuit refused to recognize this subjective expectation as a legitimate objective expectation that should be recognized by the courts. It stated, "We do not believe that an expectation that information lawfully in the possession of a government agency will not be disseminated, without a warrant, to another government agency is an expectation that society is prepared to recognize as reasonable."[22]

A long-standing refusal of the Supreme Court to extend any Fourth Amendment protection to foreign nationals residing overseas is an articulated price for security that the Court is unwilling to alter on its own. It bluntly stated:

> For better or for worse, we live in a world of nation-states in which our Government must be able to function effectively in the company of sovereign nations. . . . Situations threatening to important American interests may arise half-way around the globe, situations which in the view of the political branches of our Government require an American response with armed force. If there are to be restrictions on searches and seizures which occur incident to such American action, they must be imposed by the political branches through diplomatic understanding, treaty, or legislation.[23]

Lower Overhead vs. Clients' Rights?

While practitioners in international law might be surprised to learn that the U.S. government might well be an uninvited party to their communications with foreign clients, international clients cannot protest encroachment of rights that they never enjoyed in the first instance. However, U.S.-based attorneys representing U.S. clients should think long and hard about sacrificing those clients' rights against government privacy intrusions in the pursuit of lower overhead costs.

Some commentators have responded nonchalantly to the prospect that the U.S. government might gain possession of client information.[24] Yet once an attorney voluntarily transmits data to foreign nationals who lack Fourth Amendment protection, that attorney invites significant kinds of complications for clients. To best understand such complications, imagine an attorney who, in responding to a litigation opponent's discovery request, served responsive documents upon her client's adversary and then gratuitously made copies of everything produced for the opposing party, packed these materials up in a crate, and had them delivered to the Department of Justice, the Securities and Exchange Commission, or the Internal Revenue Service. Or imagine an IP attorney who, in response to a client's request that he prepare a patent application for a phenomenally innovative tracking radar, made copies of all his client's secret proprietary information for his

IP associate attorney or paralegal and then delivered a complete copy of that information to the Department of Defense. A client would be justifiably outraged were such a lawyer to heap such an information windfall upon the government. Still worse would be the prospect of the attorney delivering to the government all manner of undiscoverable attorney work product and attorney-client privileged information.

When attorneys outsource litigation preparation tasks, highly sensitive proprietary information, or attorney-client privilege reviews to foreign nationals residing overseas, they run the risk that lawful NSA intercepts of such information might well be transferred to agencies of the Federal Government to the detriment of their clients. While it might be the case that the attorney-client privilege survives NSA's intercept under 19 U.S.C. § 2517(4)—a questionable proposition given that the communication has been shared with third-party nationals who lack even rudimentary Fourth Amendment rights—the *evidentiary* privilege that might exist only bars the introduction of intercepted data in a civil or criminal proceeding. The privilege does not bar the government's *possession* of the information or its use other than as admissible evidence.

Given that electronic transmissions to foreign nationals overseas are "shared" with the NSA, that NSA has full rights and authority to share such information with other agencies of the U.S. government, and that the U.S. government routinely shares intercepts with the governments of the United Kingdom, Canada, Australia, and New Zealand, the transmission of electronic data to foreign national LPOs significantly implicates a client's reasonable expectation of privacy. Thus, the ability to safeguard client secrets or confidences is significantly diminished where such client confidences or secrets are electronically transmitted to foreign nationals residing overseas.

Recognizing the difficulties encountered in preserving such confidences across international borders, the American Bar Association's Standing Committee on Ethics and Professional Responsibility issued its Formal Opinion No. 08-451 of August 5, 2008, *Lawyer's Obligations When Outsourcing Legal and Nonlegal Support Services*. It states that

> where the relationship between the firm and individuals performing the services is attenuated, as in a typical outsourcing relationship, no information protected by Rule 1.6 may be revealed without the client's informed consent. The implied authorization of Rule 1.6(a) and its Comment [5] thereto to share confidential information within a firm does *not* extend to outside entities or to individuals over whom the firm lacks effective supervision and control.[25]

The ABA's legal ethics opinion of August 5, 2008, represents the high-water mark with respect to steps to be taken to safeguard client secrets and confidences when considering the use of LPOs. It suggests, for example, that attorneys actively investigate prospective LPOs prior to engaging services and that they require LPOs to conduct conflicts checks and solicit far more client input into the decision to engage LPOs. However, no ethics committee has addressed issues related to the waiver of Fourth Amendment rights with respect to electronic transmissions.[26] Should a court declare that electronic transmissions to foreign nationals residing overseas do effect a waiver of Fourth Amendment rights, legal ethics committees will certainly have to incorporate such a finding into their analysis of outsourcing ethics. As the Bar of the City of New York Committee on Professional and Judicial Ethics has stated, "each situation is different." The determination of whether an attorney's oversight and protocols are *actually* adequate will likely only be fully resolved in the context of a future-filed legal malpractice lawsuit. Just be sure that is not *your* name that is featured in the upper left-hand corner of the complaint that addresses such issues. ■

Endnotes

1. Thomas Friedman, The World Is Flat 10 (2005).
2. *See* Boumediene v. Bush, 128 S. Ct. 2229, 2260 (2008).
3. *See generally* United States v. Verdugo-Urquidez, 494 U.S. 259, 275 (1990); *Boumediene*, 128 S. Ct. 229.
4. "Maximizing billable hours is paramount and particularly challenging for lawyers affiliated with small firms or working as solo practitioners . . . . For this reason, outsourcing in the legal industry has become an established practice." Ken Wollins, *Outsourcing Legal Services Overseas: Choosing the Solution That's Best for You*, Bus. L. Today, Nov.–Dec. 2007, at 61. "In 2005, Forrester Research projected that U.S. legal jobs would move overseas from an estimated $70 million spent [in 2006] to a cumulative total of nearly 80,000 jobs filled offshore by 2015 to establish a $4 billion market." *Id.* at 63.
5. Chris Carr & Larry Gorman, *The Revictimization of Companies by the Stock Market Who Report Trade Secret Theft Under the Economic Espionage Act*, 57 Bus. L. 25, 27 (2001–02).
6. *Id.*
7. Susan W. Brenner & Anthony C. Crscenzi, *State-Sponsored Crime: The Futility of the Economic Espionage Act*, 28 Hous. J. Int'l L. 389, 390 (Spring 2006).
8. Press Release, ASIS Int'l, U.S. Companies Lost up to $59 Billion in Proprietary Information and Intellectual Property, http://www.asisonline.org/newsroom/pressReleases1093002trends.xml (last visited Jan. 27, 2006).
9. *Software Firm Attacks India's Legal Protection*, Outlaw.com, Aug. 27, 2004, http://www.out-law.com/page-4840.
10. Id.
11. Vir Singh, *Mudslinging in Indian IP Theft Case*, IEEE Spectrum Online, Oct. 2004, http://staging.spectrum.ieee.org/oct04/4028.
12. Scope of Foreign Filing Licenses, 73 Fed. Reg. 42781(July 23, 2008) (emphasis added).
13. *Id.*
14. *See* 18 U.S.C. § 2511(f): "Nothing contained in this chapter . . . shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications . . . ."
15. Erin L. Brown, *Echelon: The National Security Agency's Compliance with Applicable Legal Guidelines in Light of the Need for Tighter National Security*, 11 CommLaw Conspectus 185 (2003).
16. *Id.* at 187–88.
17. *See* Brown, *supra* note 15.
18. 691 F.2d 272 (6th Cir. 1982), cert. denied, 464 U.S. 863 (1983).
19. *Id.* at 275.
20. *Id.*
21. *Id.* at 278.
22. *Id.* at 279.
23. United States v. Verdugo-Urquidez, 494 U.S. 259, 275 (1990).
24. *Apparently NSA Reviews Offshored Legal Work!*, http://legallyours.blogspot.com/2008/05/apparently-nsa-reviews-offshored-legal.html.
25. ABA Comm. on Ethics and Prof'l Responsibility, Formal Opinion No. 08-451, at 5 (2008).
26. *See, e.g.*, The Association of the Bar of the City of New York Committee on Professional and Judicial Ethics, Formal Op. 2006-3, August 2006; San Diego County Bar Association, Formal Ethics Op. 2007-1, which lacks any analysis of Fourth Amendment waivers.