DEVORE & DEMARCO LLP
ATTORNEYS AND COUNSELORS AT LAW

CLIENT ALERT:
CORPORATE STRATEGIES FOR AVOIDNG YOUR OWN WIKILEAKS NIGHTMARE

To Our Clients and Friends:

The disclosure and mass publication of classified government documents and diplomatic cables on the WikiLeaks websites has riveted public attention throughout the world. It has also prompted considerable fear among companies and other organizations as reports emerge that WikiLeaks supporters and others are actively targeting these organizations in addition to government entities. As recent events involving the disclosure of information related to the U.S. Chamber of Commerce and a leading law firm have shown, no organization is immune from the "WikiLeaks phenomenon." In response, many companies have begun to prepare a response plan for such potential disclosures and to review their own policies to ensure that private documents and communications are appropriately safeguarded and not widely disseminated on the Internet.

Unfortunately, traditional litigation responses offer few remedies against those who are not themselves the thieves of information. First Amendment protections as well as a number of laws typically absolve websites and other downstream republishers from legal liability when they are engaged in the dissemination – but not the collection – of proprietary documents and information. Indeed, the government's inability to prevent the publication and republication of the WikiLeaks documents highlights this fundamental fact. As a result, corporations and other organizations are well-advised to focus on their own internal information privacy and security policies and practices to prevent the online dissemination of their sensitive information documents. In doing so, they should consider the following critical data privacy and security principles:

***1. Know where your data is located*:** While this is often an easy question to ask, it is often difficult to answer. This challenge is only further exasperated by the increasing use of "cloud computing." Yet knowing the location of company data is the critical first step to understanding (1) how it is secured from external threats such as hackers, viruses, sharing software, and rogue employees; and (2) which files and documents are most important -- and potentially damaging -- to the organization if disclosed and therefore require the highest degree of protection and security.

***2. Know who has access to your data*:** Understanding who has access to company data is an essential tool for ensuring that the right people have access to the right data at the right time. All too often, company information is stolen or improperly disseminated because of improper (or failed) access controls and system configurations. Having a better understanding of who can

access company information and, more importantly, how they can copy, print, transmit or alter that information, is a critical tool to avoiding unwanted disclosures. It can also help company personnel to craft appropriate and robust confidentially and non-disclosure agreements.

***3. Train those with access to your data on privacy and security best practices and policies*:** While corporations are becoming increasingly sensitive to the tremendous threats posed to company data, many employees -- not to mention third-parties such as consultants and vendors -- are often unaware of both their obligations to the data owners and the risks associated with their behavior on and off-line. Instituting training programs for all those who have access to your data can help to create a corporate culture that respects data security and, in so doing, greatly reduce the risk of a data spill. Moreover, periodic audits and compliance programs can help to ensure that those who have access to your data are continually learning and following best practices.

***4. Implement appropriate and lawful data monitoring technologies and policies*:** Some organizations may significantly benefit from actively monitoring data movement through their systems and may choose to deploy software specifically designed to detect and prevent data exfiltration. Watermarking technologies may also help companies to back track data breaches and take appropriate action against any wrongdoers. Management should note, however, that such technologies have significant limitations and can even implicate criminal liability as well as a constellation of privacy-related torts. Accordingly, before employing any such technologies, an organization must ensure that its monitoring program is lawful and is conducted with the appropriate level of knowledge and consent of those monitored.

5. Prepare for a data spill: While most large organizations have a strategy in place to cover a system outage, many still do not have a plan for handling a major data breach or spill. Such a plan focuses less on technical solutions, and instead creates a specific "order-of-battle" for dealing with the legal, regulatory, insurance, business and public relations ramifications associated with a critical data spill. The plan can be simple or complex, depending on the organization. The key, however, is to ensure that there is a written strategy in place that clearly sets out the company's and its employees' roles and responsibilities during such an event. Indeed, experience shows that organizations that have such plans are able to handle data breaches more efficiently and cost-effectively then companies who are unprepared to handle such a crisis.

While the WikiLeaks phenomenon may be new, it has always been a cardinal principle of information privacy and security best practices that no computer system is impenetrable and no internal document or data isever completely secure from external view. Understanding the principles outlined above – and acting upon them – can significantly reduce the risk of your organization being the next WikiLeaks victim.

SPECIAL NOTE*: On May 2, 2011, Joseph V. DeMarco will lead a discussion with The New York Times Company's Vice President and Associate General Counsel David E. McCraw on "WikiLeaks" and "WikiWars": Litigation Responses And Beyond. For further information, please click on the following link:
http://www.nysba.org/AM/Template.cfm?Section=Events1&Template=/Conference/ConferenceDescByRegClass.cfm&ConferenceID=4785

*This article is for general informational purposes only and should not be construed as legal advice.