LATHAM & WATKINS LLP

Spyware: The Latest Cyber-Regulatory Challenge

Berkeley, CA
April 1, 2005

Managing The Risks of Spyware: A Practical Perspective

Tim Ehrlich
tim.ehrlich@lw.com
(650) 463-2668

Overview

- Increased engagement of legal counsel by corporations relating to spyware issues
- Three primary scenarios:
  - Companies that provide spyware-like software
  - Companies that contract with “adware” or “anti-spyware” software providers
  - Companies being harmed by spyware software on an economic, IP or competitive level
- Summary

Common Reasons for Engagement of Legal Counsel

- Legislation
  - With the advent of new anti-spyware legislation at the state and federal level, a wide range of companies have or could become subject to laws regulating the use of their monitoring software
  - Seek guidance on application of new laws to current and future practices; risk mitigation strategies
- Lawsuits
  - Companies that have used, distributed and/or publicly criticized spyware/adware software have been subjected to a lawsuits from other companies and regulatory agencies on a variety of different theories, such as unfair competition, tortious interference with contract and trade libel
  - Companies harmed by spyware in the form of trademark infringement/dilution, anti-competitive behavior, economic harm
  - Seek guidance and representation on litigation and/or settlement strategies

Common Reasons for Engagement of Legal Counsel *(Continued)*

- Corporate Transactions
  - Companies seeking to protect themselves from the risks of doing business with advertising software providers and anti-spyware software licensors
  - Seek assistance with contractual negotiations and drafting
- Best Practices / Industry Groups
  - Concerns over legal, financial and reputational risks associated with spyware have motivated some companies to seek guidance on the establishment of clear internal guidelines and participation in the creation of industry best practices

Avoiding the Spyware Label

- Definition of “spyware” is not clearly established either in industry parlance or anti-spyware legislation
- Consequently, software that has certain features / functionality could fall within the classification of “spyware”
  - WhenU? Claria? DRM solutions? Other?
- Falling within that classification could have a significant negative impact on the company’s business

Avoiding the Spyware Label

- For companies that fall within the “spyware” category, some of the risks include:
  - Litigation: a variety of claims have already been brought by companies against alleged spyware providers for harm caused to their business, including trademark / copyright infringement and unfair competition
  - Criminal and Civil Penalties: State and federal anti-spyware legislation punish violators with fines and in some cases prison terms
    - H.R. 29: would impose fines of up to $3M for violations
  - Harm to Reputation: Legitimacy in the personal information / monitoring software industry is crucial to a company’s success in order to maintain its customer base and gain credibility in the eyes of perspective business partners

Risk Mitigation Strategies

- End user license agreements and privacy policies should be as clear and as up-front as possible, especially terms related to notice, disclosure policies and securing user consent
- Software installation should be very obvious and should also be easy to uninstall; make sure clear instructions and notice are provided
- Consistently monitor your practices in order to ensure they actually comply with your advertising and privacy policies
- Where software is bundled and distributed with third party software (e.g. file sharing software), establish clear standards for acceptable behavior through contractual terms and monitor on a consistent basis
- Stay abreast of legislative developments and, in particular, their application to specific categories of software

Risks by Association

- Companies that contract directly with spyware/adware companies for Internet advertising could be subject to liability/lawsuits/harm to reputation for the actions of their software/service provider
  - e.g., *WeightWatchers.com, Inc. v. DietWatch.com, Inc.* (SDNY June 2002)

- Companies that partner with anti-spyware providers or license-in their technology could wind up as a party to suits brought by:
  - Companies alleging trade libel, trade disparagement and tortious interference as a result of characterizing their software as spyware
  - Individual consumers whose computers were damaged by the removal of spyware software from their computers

Risk Mitigation Strategies

- Companies contracting with adware providers should investigate their practices before signing the contract
  - Look for deceptive trade practices and use of trademarks as keywords to trigger their advertising
- Companies contracting with anti-spyware providers should require them to establish and maintain clear classifications and appeals processes for entities marked as spyware
  - Lowers the risk of trade libel and tortious interference claims
- In both scenarios, companies should include contractual provisions that:
  - Commit their partners to engage ethically, diligently and in compliance with all laws by contract
  - Give them the right to audit their partners' business practices
  - Require indemnification for claims from consumers and other companies arising out of violations of law, privacy regulations or internal corporate policies

Economic Harms of Spyware

- Reduced profits for computer retailers and internet service providers forced to handle lengthy service calls assisting customers with spyware problems
- Harm to reputation and overall sales for computer hardware and software providers due to consumer confusion as to the source of their spyware problem
- Loss of employee productivity caused by a slow down in corporate computers and time spent resolving technical issues with internal support team
- Trademark dilution/infringement and loss of contractual relationships caused by spyware's placement of competing brands over another company's website

Risk Mitigation Strategies

- Develop or license-in a robust anti-spyware software solution, and require installation on all corporate computers
- Establish firewalls and website policies restricting employees' access to websites likely to contain spyware
- Vigorously police placement of pop-ups over websites, and consider litigation or report unfair behavior to the FTC or other regulatory agencies
- Keep your consumers informed by providing information as to what spyware is, where it comes from and how to best prevent it

Summary

- As spyware/adware/malware programs have expanded their reach, we have seen a marked increase in requests from companies to help them manage the risks associated with this technology
- Common scenarios include:
  - Companies wishing to avoid being labeled a spyware company
  - Companies that want to partner with adware or anti-spyware companies
  - Companies looking to minimize the impact of spyware on their business
- Given the speed with which the relevant technologies and anti-spyware legislation are changing, companies are encouraged to work closely with their counsel to stay abreast of new developments and to develop solutions that are well-suited to their specific business model

Although this seminar presentation may provide information concerning potential legal issues, it is not a substitute for legal advice from qualified counsel. The presentation is not created or designed to address t unique facts or circumstances that may arise in any specific instance, and you should not and are not authorized to rely on this content as a source of legal advice and this seminar material does not create any attorney-client relationship between you and Latham & Watkins.