MAYER·BROWN

Competitive Intelligence Acquisition and Reverse Engineering

Pitfalls and Best Practices in the US, the UK and Germany

Richard M. Assmus

Andrea C. Hutchison

Dr. Ulrich Worm

Sangeeta Puran

May 20, 2010

Mayer Brown Speakers

- Richard M. Assmus
  - Partner, Chicago
  - +1 312 701-8623
  - rassmus@mayerbrown.com

- Andrea C. Hutchison
  - Associate, Chicago
  - +1 312 701-8516
  - ahutchison@mayerbrown.com

- Dr. Ulrich Worm
  - Partner, Frankfurt
  - + 49 0 69 79 41 2981
  - uworm@mayerbrown.com

- Sangeeta Puran
  - Associate, London
  - + 44 20 3130 3294
  - spuran@mayerbrown.com

Topics for Discussion Today

- What we mean by “Competitive Intelligence”
- Potential US legal theories
- Special notes on reverse engineering
- Instructive US cases
- Considerations in the UK
- Considerations in Germany
- Suggestions for written CI policies
- Practical tips

Goals of the Presentation

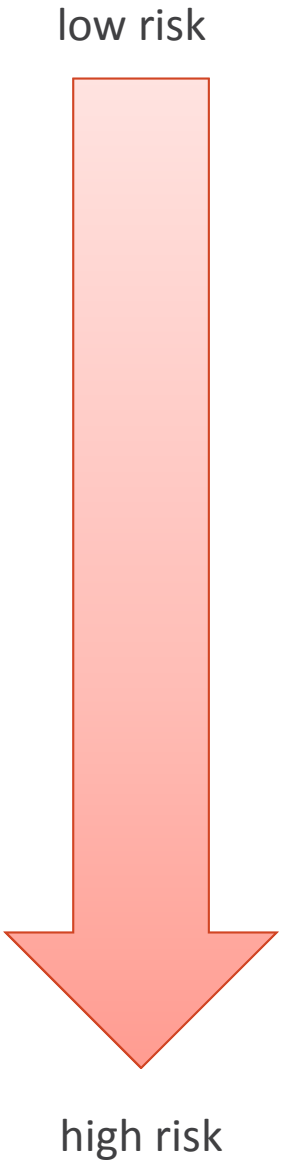
- Heighten your awareness of red flag issues, legal and ethical
- Enable you to approve reasonably aggressive CI activity, but with appropriate risk mitigation
- Familiarize you with potential causes of action in the US, the UK and Germany
- Arm you with several practical tips

What is Competitive Intelligence?

- Any activity designed to gather or analyze information regarding the competitive environment, including customers, competitors or the market
  - Activities can range from the mundane (reading an annual report) to the complex (de-compiling software); likewise, CI runs from the tame to sharp practice
  - A vast middle ground exists between these extremes
- Companies that can execute an aggressive CI strategy cognizant of the legal risks will have a competitive advantage

Examples of Competitive Intelligence

- Regular review of public statements, regulatory filings and other public and semi-public sources
- Direct observations of competitors
  - Trade show visits and other industry events
  - Price surveillance and reporting
- Competitive product acquisition, including reverse engineering
- New employee interviews / strategic hiring
- Competitor customer surveys and interviews



General Legal Risks in the US

- Done improperly, CI gathering can trigger liability under several theories:
  - Breach of employment, non-competition or non-disclosure agreement
  - Breach of product terms & conditions (*e.g.*, a product software license)
  - Tortious interference with contract
  - Unfair competition
  - Copyright infringement
  - Trade secrets misappropriation (particularly, use of improper means to obtain information)

Special Considerations for Reverse Engineering

- US Supreme Court (*Bonito Boats, Inc.*, 489 US 141)
  - "[T]rade secret law does not offer protection against discovery by fair and honest means, such as by **independent invention**, **accidental disclosure**, or by so-called **reverse engineering**, that is by starting with the known product and working backward to divine the process which aided in its development or manufacture."
- A product developed through reverse engineering remains subject to third party IP rights
- Even if IP rights are clear, the distribution of the product could be challenged as a result of a tainted development process

Special Considerations for Reverse Engineering (cont.)

- Reverse engineering involving software is a special case
  - Very likely to involve contractual issues in software licenses
  - May require circumventing software access control devices, either to access other software or to fully test a device
- The Digital Millennium Copyright Act provides a limited safe harbor for software reverse engineering incident to achieving inter-operability of computer programs
  - 17 U.S.C. § 1201(f)(1)-(3)

Trade Secrets Cause of Action

- A "trade secret":
  - (1) is **sufficiently secret** to **derive economic value**, actual or potential, from not being generally known to other persons who can obtain economic value from its disclosure or use; and
  - (2) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy or confidentiality.
- Defenses to misappropriation (*i.e.* improper means):
  - Reverse engineering of a properly acquired product
    - Publicly sold, no misrepresentation or fraud
  - Independent development
    - More complicated if a former employee has been hired or consulted

Wyeth v. Natural Biologics (8th Cir. 2005)

Facts: Wyeth's PREMARIN® for menopause is derived from a natural source —the urine of pregnant horses.

- Wyeth's extraction process was a trade secret.
- NB claimed independent development.
  - Wyeth's expired patents and literature
  - Waste manifests of one of Wyeth's plants
- NB collaborated with scientists and pharmaceutical companies and a former chemist employed by Wyeth.
- No one had previously succeeded in legally duplicating Wyeth's extraction process.

Wyeth v. Natural Biologics (continued)

- Wyeth brought suit against NB alleging trade secret misappropriation under the Minnesota Uniform Trade Secret Act.
- Outcome: Defendant NB acquired Wyeth's trade secret through improper means.
  - The plaintiff's secret was so unique that the mere "emergence of a similar, slightly altered product gives rise to an inference of misappropriation," even absent a showing of direct access to the trade secret.

Wyeth v. Natural Biologics (continued)

- Facts Supporting the Court's Reasoning:
  - NB attempted to conceal that it had been communicating with Wyeth's former chemist for ~ 1.5 years.
  - NB had financial motives for copying Wyeth's process.
  - The two processes were similar.
  - NB had no experience in chemistry.
  - NB failed to establish a credible record of how it developed its extraction process.
  - Evidence of independent research and development was "irrelevant" because of NB's conduct.

Davidson & Assocs. v. Jung (8th Cir. 2005)

- Facts: Blizzard creates and sells software games for PCs.
  - Blizzard launched Battle.net, a 24-hour online gaming service.
  - Most Blizzard games have a "CD Key."
  - Users must accept an end-user license agreement and terms of use to play the games → anti-reverse engineering clauses.
- Defendants developed the bnetd.org program.
  - No CD Key authentication
- Blizzard sued Jung et al. for breach of contract, circumvention of copyright protection system, and trafficking in circumvention technology.

Davidson & Assocs. v. Jung (cont.)

- To invoke the DMCA reverse engineering software defense, a party must show:
  - It lawfully obtained the right to use a copy of a program;
  - The information gathered as a result of the reverse engineering was not previously readily available to the person engaging in the circumvention;
  - The sole purpose of the reverse engineering was to identify and analyze those elements of the program that were necessary to achieve interoperability of an independently created computer program with other programs; and
  - The alleged circumvention did not constitute infringement.

Davidson & Assocs. v. Jung (cont.)

- Outcome: The 8th Circuit Court affirmed summary judgment in the plaintiffs' favor.
  - EULA and TOU agreements were enforceable.
    - Defendants waived "fair use" defense.
    - The agreements did not constitute copyright misuse.
  - Defendants violated the DMCA's anti-circumvention and anti-trafficking provisions.
  - The DMCA's interoperability exception did not apply.

Legal risk - UK

- Infringement of intellectual property rights
- Breach of contractual terms
- Breach of confidence under English law:
  - The information has the necessary quality of confidence
  - The information has been imparted in circumstances importing an obligation of confidence
  - There has been an unauthorised use of that information

Legal risk for reverse engineering - UK

- Reverse engineering is permitted provided:
  - No infringement of intellectual property rights
  - No breach of contractual terms binding on the reverse engineer
  - No breach of confidence

Reverse engineering and breach of confidence - UK

- General position:
  - Rights in confidential information will not prevent reverse engineering if the product has been acquired lawfully
- Lawful acquisition of information embodied in a product:
  - where product is on the market and anyone can buy it
  - even where product contains some form of encryption and reverse engineering involves de-encryption

Local Country Rules: Germany

- Under German law reverse engineering is legitimate, unless:
  - The technology to be reverse engineered constitutes a business secret;
  - the product has been obtained unlawfully;
  - the reverse engineering is accompanied by purposeful "poaching" of the competitor's employees for purposes of interfering with the competitor's business;
  - the reverse engineering leads to a product which can be qualified as a copy of the product which had been reversed engineered; or
  - the reverse engineering exercise or result infringes third party IPR.

Local Country Rules: Germany

- General rule:
  - Technology incorporated in products loses its capacity as a business secret as soon as the product becomes publicly available;
  - However, reverse engineering which requires "substantial investments" might still be regarded as trade secret misappropriation.
- Problematic, if product to be reverse engineered has been obtained unlawfully; especially
  - handling of stolen goods; or
  - aiding and abetting the unlawful act.

Local Country Rules: Germany

- It is unlawful to “poach” a competitor’s employees to interfere with the business of the competitor.
- The resultant product (as well as development activities) could infringe a competitor’s IP rights, even if the reverse engineering is otherwise legitimate — especially if the reverse engineering leads to a product which can be qualified as a copy of the product which had been reverse engineered.

CLE Code

Written CI Policies

- Why have a written policy?
  - To sensitize business actors to the legal risks
  - To guide CI activities, particularly in the formative stages
  - To memorialize institutional knowledge
  - To empower in-house counsel to say “No”
  - If needed, to dispel arguments regarding patterns of improper behavior

Sources: SCIP, law firms, in-house counsel networks

Written CI Policies (cont.)

- Suggestions for implementing a written policy:
  - Avoid legal jargon / keep the policy relatively short.
  - Ensure that policy specifically applies to business employees and those acting on behalf of the company.
  - Make third party CI vendors aware of the policy.
  - Incorporate policy into employee manual, new hire orientation.
  - Incorporate CI training into the compliance training rotation, particularly for employees on the front line of business intelligence.
  - Evaluate compliance.

Practice Points for Competitive Product Acquisition

- Document competitive product acquisition, including that the product was acquired (1) in good faith (2) from a legitimate source and (3) for fair market value.
- Maintain records to show independent development.
- If someone at your company may have had access to another's trade secrets, utilize third parties to conduct development related to those technical issues.
  - At the very least, employ appropriate screens.

Practice Points for Competitive Product Acquisition

- Avoid communicating with former employees of a competitor regarding development.
- Understand pre-existing contractual obligations.
- Document the presence of similar ideas in the marketplace and other successful attempts to copy/reverse engineer a trade secret.

Questions & Answers

Thank you

Notice

- Mayer Brown is a global legal services organization comprising legal practices that are separate entities (the Mayer Brown Practices). The Mayer Brown Practices are: Mayer Brown LLP, a limited liability partnership established in the United States; Mayer Brown International LLP, a limited liability partnership incorporated in England and Wales; Mayer Brown JSM, a Hong Kong partnership, and its associated entities in Asia; and Tauil & Chequer Advogados, a Brazilian law partnership with which Mayer Brown is associated. “Mayer Brown” and the Mayer Brown logo are the trademarks of the Mayer Brown Practices in their respective jurisdictions.
- The materials in this presentation are provided for informational purposes only and do not constitute legal or other professional advice. You should not and may not rely upon any information in this presentation without seeking the advice of a suitably qualified attorney who is familiar with your particular circumstances. The Mayer Brown Practices assume no responsibility for information provided in this presentation or its accuracy or completeness and disclaims all liability in respect of such information.
- The Mayer Brown Practices are, unless otherwise stated, the owner of the copyright of this presentation and its contents. No part of this presentation may be published, distributed, extracted, re-utilized or reproduced in any material form (including photocopying or storing it in any medium by electronic means and whether or not transiently or incidentally to some other use of this publication) except if previously authorized in writing.

MAYER·BROWN

Competitive Intelligence Acquisition and Reverse Engineering

Pitfalls and Best Practices in the US, the UK and Germany

Richard M. Assmus

Andrea C. Hutchison

Dr. Ulrich Worm

Sangeeta Puran

May 20, 2010