

# Thou Shalt Not Steal Thy Competitor's Secrets

By Jane Hodges

published on BNET.com 3/28/2007

There's nothing unethical about competitive intelligence. Most of the time, it simply involves gathering together pieces of a puzzle that are available to anyone — if they have the time and the determination to find them. But because the search can be tedious, it's tempting to look for shortcuts to get the information you need, especially when time is tight. When that happens, legal and ethical lines are easily crossed — often with disastrous financial or public-relations consequences. There are also times when ethical ambiguities arise, particularly during face-to-face interviews. So in addition to providing tips on [the right way to gather competitive research](#), we've also compiled this list of practices to avoid.

## Pretexting

---

**What It Is:**

Approaching a source for sensitive information under a false identity or deceptive pretense.

---

**Why It's Wrong:**

It's against the law. It's also lying, and lying is bad.

---

**Potential Consequences:**

Criminal conviction, litigation, fines, or prison time.

---

As part of an effort to clamp down on leaks to the press, in 2006 Hewlett-Packard hired an outside firm that used a false identity to collect phone records of several HP directors and journalists. The discovery that HP had been involved in "pretexting" (i.e., operating under a false pretext) shined a klieg light on one of the most controversial tactics used in corporate investigations. Researchers seeking competitive data — or even data about their own company — should not 1.) make fraudulent claims about why they need data, 2.) use forged information or a forged identity to request the data, or 3.) ask a third party to pull data for them using false information. If you have any doubt about what is and is not acceptable, read the [Federal Trade Commission's explanation of the law](#).

---

## Dumpster Diving

---

**What It Is:**

Picking through garbage cans to find key paperwork and documents.

---

**Why It's Wrong:**

If you dive on private property, you could be arrested for trespassing. And, well, there's the smell.

---

**Potential Consequences:**

Embarrassment for all involved if caught and possible legal consequences depending on the Dumpster's location.

---

Would a Fortune 500 company's competitive analysis team climb into corporate trash cans to get competitive information? It happens. In 2001, Procter & Gamble staffers were accused of rummaging through rival Unilever's garbage in search of documents containing competitive information. The Dumpsters in this case were not on private property, so the public dive was technically legal. Still, Dumpster diving doesn't pass the "sniff test," according to many in competitive intelligence professionals. The question to ask yourself is: If your techniques were to end up the front page of the Wall Street Journal, would top brass be embarrassed?

---

## NDA-Busting

---

**What It Is:**

Encouraging a source to violate terms of a non-compete or non-disclosure agreement (NDA) they signed with their employer.

---

**Why It's Wrong:**

It may be their neck, but you shouldn't help them stick it out.

---

**Potential Consequences:**

If your source gets fired or sued, they may try to take you down with them.

---

Some believe that if a source inside a company shares information that violates a nondisclosure or non-compete agreement, then that's the source's decision to make. But Wendy Schmidt, a principal of the Forensic & Dispute Services team at Deloitte, says if an intelligence researcher learns that a source can't talk without violating an NDA, then it's better to find an alternative source whose NDA restrictions are different (or expired) and who can thus speak freely to the topic at hand.

---

## Acquiring Trade Secrets

---

**What It Is:**

Finding the proprietary key to a competitor's success, specifically when it's a closely guarded secret.

---

**Why It's Wrong:**

It's a federal crime to acquire or share material upon which a company's success depends.

---

**Potential Consequences:**

Legal trouble with your employer, the company in question, and possibly the Feds.

---

You might want to know why your rival's product works so well, what makes it taste so good, or how a key piece of software helps it get the job done. But if your researchers turn up the mother lode — the exact recipe for the soda, or the entire string of software code — don't include it in your report. Different companies define trade secrets differently, and trade secrets differ from patents (which require public disclosure of a process or technique) and trademarks. The [Uniform Trade Secrets Act](#) states that it is illegal to "misappropriate" a trade secret, and doing so can be punishable by fines, legal fees, injunctions, and more. The [Economic Espionage Act of 1996](#) makes theft or misappropriation of a trade secret, either for foreign powers' benefit or economic purposes, a federal crime. During summer 2006, Pepsi received a mysterious letter offering to sell the secret recipe for a new drink from Coca-Cola. Rather than take the bait, Pepsi informed Coke and the two soda giants launched investigations into the leak. In the end, the Feds accused a Coke employee and two sidekicks of stealing the formula.

---

## Paying Sources for Information

---

### **What It Is:**

Giving cash to someone who can tell you what you want to know.

---

### **Why It's Wrong:**

Unless the source is an expert whose reports or commentary are commonly purchased, it can be illegal. (Plus, paid snitches are often unreliable.)

---

### **Potential Consequences:**

Lawsuits or criminal charges.

---

David Carpe, founder of competitive intelligence and HR consulting firm Clew, says this is almost always illegal except in a few industries (such as the medical/pharmaceutical industry, where "key opinion leaders" are routinely paid for their opinions or analysis). Oracle, the California software giant, was the subject of press reports in 2000 about an intelligence operation in which agents offered to pay janitors at a lobbying firm for trash containing Microsoft-related documents. That's a far cry from paying an analyst to develop a report on a new drug's potential.

---

## Appropriating Passwords

---

### **What It Is:**

Getting customers or former employees to give you passwords to a competitor's protected networks.

---

### **Why It's Wrong:**

It's a form of information theft, akin to pretexting.

---

**Potential Consequences:**

Can be illegal, depending on who uses the passwords.

---

Former employees or current customers of a rival company may have password-level access to the company's proprietary data networks. Such individuals may provide passwords that enable intelligence researchers to tap into protected sites they couldn't normally enter. In early 2007, Oracle sued SAP, accusing its rival of stealing proprietary product data from an Oracle network by posing as Oracle customers. During a similar incident in 2004, Canadian airlines WestJet and Air Canada got into a dispute over claims that WestJet execs had used a former employee's passwords to tap into an internal Air Canada site and cull sensitive passenger data. Extensive litigation ensued, with WestJet ultimately accepting responsibility for its actions and paying a fine of about C\$15.5 million.

---

## Outing a Source

---

**What It Is:**

Naming who talked and what they said.

---

**Why It's Wrong:**

You could get your source into trouble.

---

**Potential Consequences:**

Your source could be fired or face litigation, while executives in your company may be tempted to use unethical techniques to get more information from the source.

---

Full-time competitive-intelligence researchers generally agree that individuals who provide proprietary data should not be identified, except in general terms (such as "a line manager in the Northeast division," or "a store manager planning holiday inventory"). It's natural to want to know who disclosed red-hot data, but it's essential to protect your sources — both to ensure that the source doesn't get fired and to prevent someone in your company from ending up in a potentially unethical situation. For example, an executive in your company might knowingly or unknowingly try to hire the source, or someone could try to pay the source for more information.

---