In The Infotech Age They're Less Safe Than You Think. Now A New Law Protects Them--But Watch Out. If You Learn Another Company's Trade Secrets, Even Inadvertently, It Can Land You In Jail.

Even the words sound antiquated: "trade" suggesting--what?--some leather-aproned craftsman at his bench; "secrets" conjuring up all manner of theatrical and flyblown things--sliding bookcases, invisible ink, Turkish cigarettes, wall safes, femmes fatales, and firing squads. Today, when every management consultant preaches openness and sharing, the notion of locking information in a vault sounds fatally unhip.

Yet secrets are alive and kicking, their commercial value showcased in a spate of recent suits (GM v. VW, Campbell v. Heinz, Informix v. Oracle, Dow v. GE, and Cadence v. Avant, to name but five of the best publicized), each demonstrating the extraordinary lengths to which owners now will go to protect them. Urged by business, Congress has passed new and fearsome penalties to punish trade-secret misappropriation.

The FBI reports that 23 foreign governments are systematically vacuuming U.S. corporations of their intellectual assets. The end of the Cold War did not spell an end to spying. It merely changed its focus. Foreign spooks, who otherwise would be out of work, have been assigned commercial tasks. FBI director Louis Freeh says more than $24 billion a year in proprietary information is being pinched. Victims of such theft--including GM, Intel, Hughes, and Lockheed Martin--joined director Freeh last year in telling Congress that they needed additional protections for trade secrets. They noted that at the very moment the U.S. economy is becoming more dependent on intellectual property for competitive advantage, this property is getting easier to steal. Thanks to the computer's power to copy and transmit information, intangible assets can be expropriated more easily than ever, often without arousing immediate suspicion. Reason: Nothing's missing; the original is still in place. Only later does the victim wake to find his advantage gone.

Congress listened. It responded with the Economic Espionage Act of 1996 (EEA), which for the first time makes theft of trade secrets a federal offense. Where espionage can be established, the EEA prescribes prison sentences of up to 15 years and fines of up to $500,000 for individuals. Prosecutors can seize property used in commission of the crime.
Rep. Charles Schumer (D-New York), when the legislation was up for consideration before his committee (House Judiciary), asked corporate witnesses whether this really was the "howitzer" they said they needed to repel foreign spies. Yes, they said. Last October 11, President Clinton signed the EEA into law.

Don't wave your flag too vigorously just yet. The new law clearly is a howitzer. Less clear is whom it's apt to hit. For a funny thing happened to the EEA on its way through the legislative forum: It acquired another set of penalties aimed not at Dr. Fu Manchu but at homegrown thieves: fines of up to $250,000, jail sentences of up to ten years. Says Justice Department trial attorney Peter Toren: "It really can be thought of as two separate laws."

Roger Milgrim, eminence grise of trade-secret law, author of the definitive four-volume Milgrim on Trade Secrets, and senior partner at New York City law firm Paul Hastings, dismisses the espionage component of the EEA as nothing but a "political sop," impotent against anyone protected by diplomatic immunity. Rather, thinks Milgrim, it's the domestic component of the act that's apt to put thieves in jail. Who, then, is headed for the slammer? Less likely Fu than you.

If you don't remember anything else from this story, remember this: The EEA is a bear trap you don't want clamped around your leg. How might it get there? More easily than you suppose.

For now, its safety catch is on: Toren of the Justice Department stresses that Janet Reno has promised Congress she will exercise restraint in invoking it. (And much will depend, of course, on how courts interpret it.) Nevertheless, in the opinion of James Pooley, author and partner at the Fish & Richardson law firm in Menlo Park, Cal., the EEA "has the potential to change business behaviors in fundamental ways." He might well have added, "and in rinky-dink ways too"--which, if anything, is scarier. Consider these situations:

You're on a plane. At takeoff, a report belonging to somebody a few rows up slides along the inclined floor, coming to rest against the toes of your well-waxed wingtips (or pumps, as the case may be). You pick it up, noting it's stamped CONFIDENTIAL. Hot diggity! It's a marketing report belonging to your archrivals at Nemesis Co. You gleefully digest its contents.

Same airplane, different situation: Two guys seated next to you are blathering out loud about the sales presentation they'll be making when they land, ignorant of the fact that you're the enemy and that you'll be presenting against them. You soak up every detail.

You're the head of Staples. (This example isn't hypothetical. It's taken from page 72 of Thomas G. Stemberg's 1996 exercise in braggadocio, Staples for Success.) You want to get the drop on Office Depot. So you have your wife, Dola, apply for a job at OD's delivery center in Atlanta. Dola, Stemberg writes, "had experience in telemarketing and in a soft, Southern accent, explained that she was anxious to move back 'home.' Staples did not offer delivery service at the time, so I wanted to investigate how Office Depot's delivery system worked, how many people were in the operation, and how it trained employees."

Thanks to Dola's dodge, Stemberg got his info.

Such shenanigans are now illegal. Or probably illegal, since the EEA defines theft as the knowing misappropriation of a secret without its owner's consent. Where big fines and jail time beckon, "probably" introduces an element of risk you'd be a chump not to eliminate if you could. How can you? By returning the report (in situation one) unread. By telling your garrulous seatmates (in two), "Boys, I'd shut up if I were you. I work for the competition." And by not using your wife as a spy.

Are we saying you're obligated, now, to protect competitors from their own stupidity? Yes. That's assuming you want to adopt a belt-and-suspenders approach to self-protection, and perhaps you should. Says Pooley: "Good-citizen companies are going to find themselves unexpectedly exposed to criminal prosecution."

A company theoretically can run afoul of the law simply by hiring an employee who brings with him a Rolodex from a past employer. The contacts on that Rolodex may be deemed trade secrets. If they are, and if the new hire uses them to the detriment of his old employer--watch out. Unless you (as new employer) can prove he was a "rogue" whose actions circumvented the best safeguards of your EEA-compliance program, you could be in trouble. You say you don't have a compliance program? Then
you're really in hot water. Say hello to wider pinstripes.

Before the EEA, the definition of "trade secret" was plenty broad already, able to include computer source code, the design for a golf course drainage system, the tightness or looseness with which a nut is threaded to a screw, a recipe for baked beans, another for trout bait, a process for casting metal golf club heads, and parts of a religious doctrine. Even "negative" know-how was included: blind alleys, knowing what doesn't work, what not to do.

Now it has been expanded to include, explicitly, all types of business and financial information. Here, so you can have it tattooed on your arm for easy reference, is the EEA's definition of a trade secret, in all its Grand Canyon scope:

"All forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if: (A) the owner thereof has taken reasonable measures to keep such information secret; and (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public."

Patents apply only to inventions (and only to novel, useful, and nonobvious ones, at that). Trade secrets, by contrast, can apply to mere ideas and information. Their all-inclusive nature can mislead companies into believing that everything they've got is secret. It's not, as Dow discovered to its embarrassment.

Dow sued GE in April, alleging theft of secrets concerning a Dow process for making plastic instrument panels for cars. Dow said GE had hired away 14 of its experts, including engineer Daniel Kaufman, in an attempt to steal secrets and set up a mini-Dow within GE. The suit engaged the attention of senior management at both companies, including chairmen William Stravropoulos (at Dow) and Jack Welch (GE), who at one point dealt directly by phone.

Then, eight days after filing suit, Dow backed down. Dow had believed a crucial piece of evidence proved theft: A marketing report written by Kaufman for GE contained information Kaufman could have gotten only while at Dow. Up to a point Dow was right: The information had indeed been obtained by Kaufman while at Dow. But Kaufman had obtained it from a public presentation made by officials from GE.

Ooops.

In a more recent case, software maker Informix launched a hugely vituperative lawsuit against rival Oracle, claiming that Oracle had hired away 13 workers to pluck them of their secrets. The dispute spilled over onto highway billboards, which the two companies used to hurl public insults at each other.

Then, in June, Informix announced that it had learned (through legal discovery) that Oracle had not misappropriated any of its secrets and had not disclosed any of its confidential info.

Informix "regretted," it said, having suggested anything to the contrary. It thereby so covered itself with egg that had Silicon Valley's temperature been any hotter, it could have passed muster as a Monte Cristo sandwich.

Making sure your valuable information will have trade-secret status isn't tough. An ordinary client list, for example, can be made more clearly a trade secret if it includes details known only to you—e.g., a customer's taste in cigars, Scotch, or French underwear, for example. Software company Cadence Design first suspected its source code had been snitched when a Cadence engineer recognized in a rival's product quirks he had deliberately inserted into Cadence's original.

Such steps can help you know more surely than Dow or Informix that a secret has actually been stolen. But don't blame them for moving as fast as they did. The moment an owner even suspects he's been robbed, he must act immediately, not only to appear a responsible property owner in the eyes of a court but to prevent his secret's becoming more widely known (hence worthless). Exposure does to secrets what sunlight does to vampires: It destroys them, quickly. New technology only makes destruction easier.
The Internet? It's an abattoir for secrets. In a few keystrokes, an anonymous info-terrorist, saboteur, blackmailer, nut, or proverbially disgruntled employee can publish a trade secret on the world's most public bulletin board. An enemy of the Church of Scientology did just that: posted on the Internet excerpts from secret church teachings drafted by founder L. Ron Hubbard. A court judged the secrets destroyed, since they had thus been exposed to a potential audience of some 25 million people.

The demise of the Cold War has opened up a treasure chest of snoop technology previously reserved for military use. Who'd have worried--until now--that a competitor might spy on one by satellite?

In June, Popular Mechanics, a journal usually given over to spark plug and motor oil advice, reported that the U.S. government's supersecret military installation in the Nevada desert--Area 51--had moved. Yes, the Area 51 U-Haul evidently had come and gone already, leaving behind only alkali, some Betty Grable posters, and a disconsolate small green man or two. The question PM posed was: Where had it gone? Area 51 hadn't left a forwarding address, so sleuthing was required.

The magazine asked Aerial Images, a company that sells photos snapped by satellites belonging to the former Soviet Union, for reconnaissance information on several likely spots. The company declined--but only because U.S. security was at stake. If PM's target had been private (Popular Science?), Aerial Images would not have had a problem.

Says PM writer Jim Wilson: "These satellite companies are sprouting up all over. They'll sell to anyone." Wilson eventually got the information he needed through a conventional aerial-survey company using airplanes. (Relatives and friends of Area 51 will be relieved to know it is living now in Utah under a new name: Area 6413.) Makes you hesitate to put anything too confidential on your roof.

Secret-owners must contend not only with new, high-tech threats but with old, low-tech ones rooted deep in human nature: People simply can't keep secrets. What's worse, they seem hard-wired to blurt them out. "The vanity of being known to be entrusted with a secret," wrote Samuel Johnson, "is generally one of the chief motives to disclose it." But there's a second fatal strain of vanity: pride of discovery.

Explains French-Swiss-Canadian cranberry baron Philippe Bieler: "People are delighted to tell you everything they've learned. When my brother and I were getting started in the berry business years ago, I went to Wisconsin, headquarters of the biggest growers. They told me what to do. More important, they told me what not to do. The pH of water is very important to cranberries. To be just right, you need to use bog water, not river water. Our property in Canada was alongside a river. We'd have used only that water and gotten poorer yield had our competitors not corrected us."

A few sensible policies can stop such aid to the enemy. Naomi Fine, whose company, Pro-Tec Data of San Leandro, Cal., has helped some 200 corporations guard their secrets, says someone should review all speeches and public pronouncements, especially ones made by scientists or others aglow with the pride of discovery. Press releases should be screened by product managers. Similarly, says competitive-intelligence expert Leonard Fuld, president of Fuld & Co., in Cambridge, Mass., companies frequently disclose far more information than they have to when submitting government forms. "Ask manufacturing personnel, or whoever is involved in submitting the report, to list data they'd prefer withheld," he says. "Have counsel then determine how much of this can legitimately be eliminated."

If "Keep your mouth shut" is the first law of secret-keeping, the corollary is: "And everybody else's too." Surely, though, there's more to secret-keeping than that? Makers of equipment would have you think so.

IriScan 2020, an iris-reading scanner, grants or denies a visitor access to a room by discerning, within his eyeball, a pattern quite as unique as your own thumbprint.

And speaking of your thumbprint: Let's say that tonight, while you're asleep, the agent of a shadowy foreign power sneaks into your bedroom and snips off, with pruning shears, your thumb. Rest easy. The agent can't use it to gain access to your vault--not, that is, if you've had the foresight to buy Veriprint 2000, which, by being sensitive both to pulse and skin temperature, knows a dead digit when it sees one.

If you love such gadgets, by all means get them. But legally, they're not required. Legally, you need only
satisfy a court that you took "reasonable" care protecting your trade secret. That doesn't mean you need to replicate Fort Knox. It means you need to buy a rubber stamp ($3.98) reading CONFIDENTIAL with which to mark documents.

And don't go overboard with it either. Stamping everything secret debases real secrets' value. With courts, less is often more. Burdensome, overly elaborate security programs--ones that impose, say, five different levels of confidentiality--can be counterproductive. If honored in the breach, such programs may be judged by a court to have contributed to your secret's loss. As a practical matter, laboratory personnel have been known to become so exasperated by security excesses that they have "guessed" at formulas rather than have to get clearances necessary to look them up--inviting explosive consequences.

Trade secrets don't escape on airy legs. They hitch rides on human hosts--usually on exiting executives. The owner's challenge is to keep the lips of defectors sealed while promoting the loyalty of all who remain. The solution devolves, as do so many problems of human management, to offering a carrot while brandishing a stick.

First, the stick: Asked to explain the sophisticated system governments use to maintain state secrets at the highest level, professor Christopher Andrew of Cambridge University, an authority on spying and national security, says simply: "It comes down to frightening people." With noncompete agreements unenforceable in several states (including California), and with job-hopping now virtually an Olympic sport, companies wanting to frustrate defections are pulling a special arrow from their legal quiver: a suit charging the defector and his would-be employer with misappropriation of trade secrets.

Big companies are willing now as never before to chase employees to make sure they behave. "Remember when Iacocca went to Chrysler?" asks attorney Pooley. "Nobody batted an eye. There used to be a gentleman's agreement not to sue. Now there's been a string of lawsuits based on the theory that information inevitably will be disclosed."

Companies, whether or not they lose these suits, get to use the defector the way medieval towns used heads on pikes: as a fearsome symbol saying "ixnay" to anybody else tempted to bolt.

You fervently don't want to be the targeted executive. Case in point: Daniel J. O'Neill. Until January, O'Neill was head of U.S. soup operations for Campbell. Heinz asked him to head its North American operations (and parts of South America too), so he told Campbell he'd be leaving. Campbell in effect said: Whaddaya, krazy?

The company reminded O'Neill that he had signed a noncompete agreement that forbade his working for a number of competitors, among them Heinz. It also contended he was full to the gills with soup secrets.

Well, okay, said O'Neill in effect: Heinz and I will redefine my job so that it in no way puts me in conflict with my beloved old pals at Campbell.

That wasn't mm-mm-good enough for Campbell. It argued that O'Neill (who'd attended Campbell board meetings and had been privy to Campbell's long-range plans) would inevitably spill beans, no matter what Heinz job he held. After salvos of lawsuits back and forth, the two companies (and O'Neill) worked out a compromise.

When O'Neill finally goes to work for Heinz in September (after having sat out nine months of enforced idleness, so the Campbell secrets in his brain can have gone stale), he won't be head of North America.

He won't be head of South America.

There's almost no limit to what he won't be head of.

Under the terms of the settlement, O'Neill will be permitted to work in two product areas only: tuna and pet food--categories in which Campbell and Heinz don't compete. Can he work in beans? No. Mustard? No. Pickles? No. And don't even think about soup. It's just tuna, pal. Tuna and pet food. Period.

To ensure compliance, his activities will be supervised by a "keeper" (an independent auditor from a Big
Six accounting firm, paid for by Heinz), who will review his every move: what executives he sees, whom he telephones, what factories he visits, what topics he discusses. Until the settlement expires in August 1998, O'Neill will be living the life of an Alexandre Dumas character: the man in the tuna-and-pet-food mask.

Courts in such cases face a daunting task: They must parse out the contents of the employee's head, deciding what belongs to him as part of his professional baggage, and what belongs to his employer as a trade secret. They also must decide whose right will be superior: the owner's property right or the employee's right to earn a living.

So much for the stick. Now how about the carrot?

Dorothy Young, 88, assistant to one of the greatest secret-keepers of all time, well remembers how he did it. Yes, she had to sign an oath--but all of Harry Houdini's assistants had to. It read in part: "I hereby swear by God the Almighty not to reveal in any manner to anyone, no matter who it might be, nor even to give the smallest hint, of the secrets, instructions, plans, apparatus, constructions you have confided in me in reference to the execution of your numbers."

Thanks partly to such precautions, says Houdini biographer Kenneth Silverman, many of his greatest "numbers" remain secrets to this day, even among magicians.

Dorothy Young gets to the heart of her old boss's secret-keeping genius when she recalls the "compassion, kindliness, and thoughtfulness" with which he treated her. "He and Mrs. H. really made me feel as if I were part of their family." That's your best guarantee of circumspection: employees who identify your interests as their own. "I've had so many people try to get me to divulge his secrets," muses Young. Since 1926, though, when she last saw the Master, she hasn't. Now that's a trick.