

21/5/2001

National Labor Court of Israel

Dan Frumer and Checkpoint Ltd. [Appellants]

v.

Radguard Ltd. [Respondent]

Subjects: *Freedom of Occupation, limited validity of covenants not to compete, trade secrets, individual contracts of employment, free mobility of labor, injunctions limiting employment at competitor of former employer*

Facts of the case:

Checkpoint and Radguard, both founded about four years before this hearing, are companies which develop and produce information protection systems based upon VPN (virtual private network). Radguard employs about sixty workers, while Checkpoint employs about five hundred workers, two hundred in Israel and three hundred in the U.S.A. Radguard is a small company while Checkpoint is one of Israel's hi-tech successes, with about a third of the world market in information protection and is worth about seventeen and a half billion dollars on the American stock market. Checkpoint's information protection system is called "Firewall-1", which is an integrated software system enabling the user to block his computer or network against unwanted or undesirable messages. "Firewall" has become a general term for computerized methods for protecting secrets from unauthorized users.

Checkpoint develops and produces software products which can be used on standard computers. Radguard concentrates on hardware, developing and manufacturing boards and chips (CPU); its main product is called "Cryptowall Cipro", which is an integrated system based on Radguard's hardware, used together with other companies software.

Mr. Dan Frumer is a software engineer with experience from working in the defense industry and for various companies, including Digital. With this experience under his belt he joined Radguard, being one of its first four employees and working as a senior development engineer and then director of research and development (R & D). In this capacity Frumer participated in management meetings and, therefore, knew much information about the company. He did not, however, deal with marketing. Mr. Frumer is an expert in the VPN field, with experience in software development, integration between software and hardware and managing hi-tech development teams.

When Radguard's CEO decided to remove Frumer from his position as director of R&D and did not offer him another position, he resigned, stopped working at Radguard on August 8, 1998; their employer-employee relationship ended on October 31, 1998. It is clear that Frumer did not resign because he sought or was offered a position with another company. Frumer began working for Checkpoint on November 15, 1998.

During the three months between Mr. Frumer's resignation and the formal severing of employee-employer relations with Radguard he searched for another position, with the assistance of a manpower recruitment firm specializing in hi-tech. He was offered several positions, in Israel and abroad, and accepted the one with Checkpoint as a senior development manager, managing and coordinating the work of development teams. Mr. Frumer worked with Checkpoint only two months, until the Regional Labor Court enjoined him from doing so.

The hi-tech industry is considered one of the foundations of the new world economy and especially the Israeli economy. Development of hi-tech in Israel has been rapid and has spurned sub-branches, including the information protection field. Communication between computers and networks necessitates preventing unauthorized access to data and has made information protection an important field. One advanced technology for protecting information communicated between computers is VPN (virtual private network), which permits encoding/concealing messages in networks serving many users and open to the public. VPN products integrate both software and hardware.

Decision

The Tel Aviv Regional Court, the trial court and court of first instance, granted Radguard's motion for a temporary injunction prohibiting Frumer from working for Checkpoint for a period of eighteen months, thereby reducing the twenty two month restrictive period set in the Labor contract. Checkpoint and Frumer appealed to the National Labor Court against any limitation on Frumer's freedom of occupation.

The National Labor Court quashed the injunction and held that a covenant not to compete was not enforceable, unless the worker used his former employer's trade secret at his new work, acted in bad faith or received special compensation not to compete. While Frumer's knowledge of Radguard's R&D plans was a trade secret, it was of little value to Checkpoint after nine months had passed.

Law applied

Israel has no Labor contract law. However, the **Commercial Wrongs Law of 1999** relating to trade secrets was relevant and is cited in the judgment.

JUDGMENT

Judge Stephen Adler (President) handed down the majority opinion:
The covenant not to compete

The Labor contract between Frumer and Radguard, signed May 23, 1994, contained a restrictive covenant, prohibiting him from working for a competitor for twenty two months after ceasing to work for Radguard; not to reveal Radguard's trade secrets and not to work in any position in which he would use information learned at Radguard.

Are Radguard and Checkpoint competitors?

Mr. Frumer undertook not to work for a company which competes with Radguard. Counsel for Radguard argued that covenant prohibits him from working for Checkpoint, since it competes with Radguard in the field of information protection based upon VPN. Moreover, there is a good chance that Frumer will use information and trade secrets learned at Radguard while he works for Checkpoint. Counsel for Checkpoint replied that the two companies are not competitors, since Radguard produces hardware and Checkpoint markets software.

On the basis of the facts before this court the two companies do compete in the field of information protection for networks: both develop products using the VPN system; their final products co-ordinate between hardware and software; and both offer the consumer products which perform the same function. Also, the covenant not to compete prohibits "direct or indirect" competition and, therefore, it is sufficient that the competition is the product offered consumers for the covenant to apply.

[description of the hearing in the Regional trial court.

The parties arguments]

The issues

This judgment relates to the following matters: first – Mr. Dan Frumer's (hereinafter: Frumer) right to work for Checkpoint Ltd (hereinafter: Checkpoint) and its' right to employ him; second – restrictive covenants, ie. Should the Court enforce Radguard Ltd's contractual right to restrict the above work relationship for twenty two months; third – whether Radguard has proven that Frumer's knows and will use trade secrets during his employment at its competitor Checkpoint? In this context we must determine whether Frumer's knowledge as a program engineer and director of research and development at Radguard are skills he can use wherever he works or are "trade secrets" which prevent him from working for Checkpoint.

Therefore, the following issues arise in this case:

[a] should covenants not to compete be enforced; if so, under what circumstances and what weight should be given to them?

[b] Is there a reasonable chance that Mr. Frumer will use Radguard's trade secrets during his work at Checkpoint?

[c] How should we balance the freedoms, rights and interests of the parties?

Several basic principles conflict in this case: Frumer's freedom of occupation; Checkpoint's right to employee Frumer; the parties' freedom of contract, including that of Radguard and Frumer to agree on a covenant not to compete; public interest in a free competitive market, mobility of Labor and the rapid transfer of information in the economy.

Existing case law

To reach such a balance the Court must balance these principles, determine their relative importance and apply them to the particular factual situation. This balancing of rights approach is used by the Israeli Supreme Court [citations], the German Federal Labor Court [citations] and Canadian courts, as described below:

“... the courts must strike a balance between the employee’s interest in being allowed to exploit the knowledge, expertise and skills – his or her intellectual capital, so to speak – that he or she has acquired from the job; the employer’s interest in exploiting its investment in the business; and the public interest in facilitating Labor mobility and free competition in products and services” [I.M. Christe, G. England, B. Cotter, ***Employment Law in Canada*** (Toronto, 3rd ed, 1998), p. 11.72].

Until now Israeli case law has applied balancing legal principles courts by considering reasonableness and proportionality, ie. whether the restrictions on freedom of occupation are reasonable in the circumstances, regarding the length of the restriction, its’ geographic scope, the parties’ possible injuries [citations]. This reasonableness standard is also used in some American jurisdictions, as described below:

“On the one hand, an employee cannot be prohibited from selling his knowledge and skills – including general knowledge learned and skills perfected in prior employment. There is a recognized societal interest in allowing individual freedom to practice a trade or profession and to increase the utilization of knowledge and skill ... On the other hand ... the employer’s interest in trade secrets – unique information that

gives the prior employer a competitive advantage – is also worthy of protection...

The prevailing view in most jurisdictions is that covenants not to compete are enforceable only if reasonable – and reasonableness turns upon an assessment of whether it is greater in duration, scope of employment, and geographic area than is necessary to protect the employer's legitimate interests; imposes an undue hardship on the former employee's ability to earn a living or practice a profession; and the extent to which the public interest is affected...

In some jurisdictions, a finding of unreasonableness makes the covenant totally unenforceable, on the theory that a judicial narrowing of the covenant will only encourage employers to write broader covenants hoping to trench closer to (or transgress) the line of reasonableness. Others allow the courts to 'blue pencil' the covenant, narrowing the duration, geographic scope and nature of the work, in an effort to achieve a fair balance of competing interests" [M.W. Finkin, A.L. Goldman, C.W. Summers, *Legal Protection for the Individual Employee*, (1989) West pub, pp 186-187].

British courts have adopted a similar approach:

"The courts are prepared to enforce such covenants only if the employer can show: [1] that there is a clear proprietary interest requiring protection, ie. there are genuine 'trade secrets' or confidential information involved and [2] that restraint is reasonably necessary to protect such trade secrets, ie. that there is a real possibility that the information will be improperly used or if used would have a damaging effect; and [3] that the restraints are reasonable in scope, ie no greater than is necessary to protect the proprietary interest taking into account the nature of the activities which are being restrained, the position of the employee, the period of time for which the employee is restricted and the geographic scope of the restriction". [S. D. Anderson, *Labor Law: Management Decisions and Worker's Rights* (London, 3rd ed, 1998), pp 68-69].

A similar standard also exists in Canada [citations].

The reasonableness standard is broad enough to consider protection of various employer interests, although the protected interest is usually trade secrets. Furthermore, there are various levels of legal rights; freedom of

occupation and the property right are constitutional rights in Israel. On the other hand, covenants not to compete are contractual obligations. Trade secrets are intellectual property and relate to the constitutional property rights.

Why an employees' freedom of occupation should not be limited

Mr. Frumer's contractual obligation not to compete with Radguard is within the parameters of the parties' freedom of contract and Radguard's intent to protect its' trade secrets. However, restrictions of the freedom of occupation also relate to public interests and policy supporting a free competitive economy. This has been expressed by a British Court:

“... an employer has no legitimate interest in preventing an employee, after leaving his service, from entering the service of a competitor merely on the ground that the new employer is a competitor”. [***Kores Manufacturing Co. Ltd v. Kolok Manufacturing Co. Ltd*** (1959) Ch 108, p. 125.]

In my opinion a covenant not to compete should not be given much weight. It should be enforced only if it is reasonable and protects the former employer's trade secrets... I suggest this new standard for the following reasons:

The first reason – The Basic Law: Freedom of Occupation grants a person the right to work in any occupation, profession or craft as a constitutional right [citations]. Furthermore, human capital is important. Mr. Frumer's professional ability and expertise are his property and the source of his livelihood; they are protected by ***The Basic Law: Human Dignity and Liberty***, which makes the property right a constitutional right. The knowledge and experience which a worker accumulates in the course of his work become, in the course of time, part of his skills. This includes, among other things, the use of computer programs, work methods, formulas and equipment. A person should not be limited in using his property.

The second reason – A basic principle of employment law is not to enforce conditions in Labor contracts which a reasonable worker would not undertake from his free will. The policy arises from the presumed inequality between the power of the individual worker and his employer. Thus, we do not enforce a worker's contractual undertaking to waive rights granted by protective Labor legislation, since a reasonable worker would not waive these constitutional rights. In general, a worker seeking work has little option to refuse a covenant not to compete, otherwise he will not be hired.

The third reason – The workplace is not only a source of livelihood but also of satisfaction and self-fulfillment. Restricting a workers ability to choose his workplace curtails his right to determine his own fate. Furthermore, mobility is common in today’s economy. Workers change jobs to further their careers and improve work conditions. An employee should be free to determine when to leave a job and try to improve himself. This is apparent in Mr. Frumer’s situation, since his professional career had been sidetracked at Radguard and working at Checkpoint gave him an opportunity to use his professional expertise.

The fourth reason – The modern economy is based upon competition and free movement of capital, commodities and Labor/services. Restriction movement of a worker prevents him from obtaining the wage which he is worth on the free market; it restricts competition for human capital. Workers offer their services and compete for jobs; employers offer wages and working conditions in order to attract workers. The free competitive market benefits consumers since it generally reduces prices. Competition often encourages new businesses, including those of people who compete with their former employers.

Circumstances in which freedom of occupation can be limited

Under what circumstances can a covenant not to compete be enforced? As mentioned above freedom of occupation and free competition are not absolute rights. They must be balanced the societies' interests and those of the former employer. The society must protect the employer's property, including against a former employee who uses it illegally. This protection is mainly thru patents and copyrights. However, the employer's trade secrets are also protected. However, prior to limiting a worker's freedom of occupation the Court must consider the following:

[a] **Trade secrets** – a worker's freedom of occupation should be limited in order to prevent him from illegally using trade secrets belonging to his former employer. Trade secrets are protected by intellectual property laws and **The Commercial Wrongs Law of 1999**, which shall go into effect on October 29, 1999. Since this the

protection of trade secrets is by law a covenant not to compete is unnecessary to enforce the former employer's rights.

[b] **Special training** – If an employer financed a worker's training and in light of this special cost the worker agreed to work for him for a fixed period, his freedom of occupation can be limited. This does not apply, however, to the training which a worker receives as part of his regular work or thru his own initiative and cost.

[c] **Special consideration** – which a worker receives for his undertaking not to compete with his former employer is also a basis for limiting his freedom of occupation.

[d] **The good faith duty and loyalty obligation** must be considered when deciding whether to limit a worker's freedom of occupation. The loyalty obligation of a worker imposes a more stringent standard of behavior than does the good faith obligation. An example of a violation of the loyalty obligation is when a worker contracts with a third party to establish a business which will copy his current employer's production process [citation].

We note that the loyalty obligation is more stringent regarding senior executives. Also, the loyalty obligation and its' derivatives are in effect during the employment period and thereafter.

When the above considerations are not based upon a statute the Court will limit the worker's freedom of occupation on the condition that there is an explicit contract provision in the Labor contract between him and his former employer. However, the worker has a duty to act in good faith, even when there is no specific limiting covenant.

The above four considerations are not a closed list and the Court must determine each case upon its' facts. The rule is, however, that a covenant not to compete will not be enforced unless one or more of the above considerations exists. Furthermore, even then the Court is not compelled to limit the worker's freedom of occupation, but will decide based upon all relevant facts, principles and interests.

Protection of Trade Secrets and Intellectual Property

The protection of trade secrets can be based upon either a specific section of the law, the loyalty obligation or a contract term. [citations]. In the hi-tech industry a company's intellectual property is a very valuable assets in which much resources have been invested.

.... An injunction limiting a worker's occupation will not be issued unless the employment at the new workplace threatens the former employer's survival. The former employer must prove that the use of the trade secret will threaten his business.

Checkpoint's counsel referred us to California law, where the condition for honoring a covenant not to compete is the existence of trade secrets. Also, the former employer must prove that there is a reasonable likelihood that the worker will make use of information gained before ttd, especially a trade secret [citations of the California Business and Professions code, sections 16600-16607; Unfair Practices Act, Section 17300]

The Definition of a Trade Secret

How are we to define a “trade secret” and does it include the knowledge which an employee learned in the course of his work? Section 5 of the **Commercial Wrongs Law** defines states:

“5. ... ‘trade secret’, ‘secret’ – commercial information, of any type, which is not public knowledge and cannot be discovered by others, which gives its owners a commercial advantage over others, if its’ owners take reasonable precautions to guard the secret”.

Thus, we are dealing with a trade secret when the information is known only to the employer, is not common knowledge and cannot be easily discovered. Generally, a companies’ trade secret is known to a small circle of employees, such as the senior management of the marketing manager.

Much information can be discovered by modern communication methods, such as the internet. All employees of many companies receive much information on the company. Such information is not a trade secret. Information which is available to the public, or sold to the general public, is not a trade secret.

We should emphasize that the definition of a trade secret differs by industry or economic branch.

Moreover, when defining “trade secret” we must take the public good into consideration, including its’ right to know and whether making it common knowledge will benefit the public. Sometimes this consideration can outweigh those protecting the property rights of a trade secret.

We can also learn about the definition of a “trade secret” from the law of other countries. In the United States the Uniform Trade Secrets Act defines “trade secret”, as follows:

“ ‘Trade secret’ means information, including a formula, pattern, compilation, program, device, method, technique, or process, that: derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure, or use, and is the subject of efforts that are reasonable under the circumstances to maintain secrecy”.

Section 757 of the Restatement of Torts states the considerations which are guidelines for determining whether a specific information is a “trade secret”:

- “(1) The extent to which the information is known outside the company’s business.
- (2) The extent to which the information is known by employees and others involved in the business.
- (3) The extent of measures taken by the company to guard the secrecy of the information.
- (4) The value of the information to the company and to the company’s competitors.
- (5) The amount of effort or money expended by the company in developing the information.
- (6) The ease or difficulty with which the information could be properly acquired or duplicated by others”.

.... [citation: Section 3426.1(b) of the California Civil Code]

Examples of “trade secrets” in American case law are: a list of customers or suppliers which was prepared and kept secret by the employer; business plans, formulas and designs; computer programs and information. General knowledge, such as methods of operating known computer programs, which are common knowledge, are not considered trade secrets.

What is a “trade secret” in the hi-tech industry? An important American researcher in this field answered the question as follows:

“... a trade secret in Silicon Valley consists of a program, protocol, or design blueprint that exists in tangible form, such as a document or diskette, previously clearly marked as confidential and proprietary, never published or revealed to the trade, but nevertheless removed, downloaded, or emailed from the old employer without his consent”
[A. Hyde, “How Silicon Valley Effectively Abolished Trade Secrets”].

It is not enough to claim that a “trade secret” exists, the former employer must prove this, by describing it in detail. It is insufficient for him to argue in general terms, as was done in this case and, for example, he must prove a specific: computer program, formula, design, customer list or process, etc. When putting forth such proof one must relate to the extent of the trade secret and how long it can remain a “secret”. The former employer must also prove that the information is “secret” and that he has taken proper

measures to protect its' secrecy, such as revealing it only to employees who need the knowledge for their work and keeping it secret from other employees, or keeping the secret in a secure place.

We are aware of the problems relating to protecting "trade secrets" during the legal proceeding. However, courts have the tools to do so, such as closed door hearings.

Also, the level of proof in a hearing for a temporary injunction, such as this case, consists of preliminary evidence. However, since the main hearing can last a few months the decision in the temporary motion can determine the workers and employer's fate. Therefore, even though we are dealing with a temporary injunction, the court should require detailed proof of the trade secret.

Does Dan Frumer have a "trade secret" belonging to Radguard?

The main claim of Radguard's attorney was that knowledge which Frumer learned during his employment at Radguard will benefit him at important stages of his supervisory work at Checkpoint. It was also claimed that Frumer could use such information for developing hardware performing similar functions as Checkpoint's software. These claims were not proven in the hearing relating to the temporary injunction.

Knowledge which is not a "trade secret"

The basic rule is that knowledge, information and experience which an employee learns during his employment becomes part of his qualifications and experience and he is free to do with it as he pleases. When an employee begins a new job he is not required to forget all such information and experience; as long as he does not use his former employer's trade secrets. Justice Strasbourg-Cohen expressed this as follows:

"In general, when employee-employer relations have ended, the worker is free to use his personal work qualifications and knowledge and benefit from them, including to compete with his former employer, so long as he does not use his former employer's 'confidential' information, which use would be a violation of his duty of loyalty and good faith behavior."

This rule can also be derived from Section 7(a) of the **Commercial Torts Law**, which states:

"(a) A person shall not be liable for stealing a trade secret, if one of the following exists:

- (1) The information embodied in the trade secret became known to him during his employment by its' owner and

- this knowledge became part of his general professional qualifications;
- (2) Using the trade secret is justified for the public benefit”.

For example, an attorney employed in a law firm, previously studied law and worked in another firm; in his current employment he broadens his knowledge and expertise. This does not prevent the attorney from resigning and using his professional experience in another firm, even if the new firm specializes in the same field. Another example is the carpentry apprentice who is free to open his own competing carpentry business. However, this apprentice is prohibited from copying a design/model which his former employer developed...

Regarding the stages of research and development of computer programs, such as those involved in this case, Prof. Bornovsky has said:

“... when a competing computer program developer does not copy a specific end result but copies the stages of logic and requirement definitions, whose essence is the development and implementation of ideas, or is assisted by them, or relies upon them, it is doubtful whether intellectual property protections apply, since the basic rule is that they do not protect ideas but end results”.

To deepen our knowledge of trade secrets in the hi-tech industry we studied writing of American academics... The American rule is, as follows:

“Courts also recognize that knowledge, skill, expertise, and information acquired by an employee during his employment become part of the employee’s person. They belong to him as an individual for the transaction of any business in which he may engage, just the same as any part of the skill, knowledge and information revived by him before entering the employment”. [von Kalinowski, “Key Employees and Trade Secrets” 47 Va. L. Rev (1961), p. 586.]

In the context of determining rights to inventions by employees, which are based upon general information learned from a former employer, American case law states:

“[A former employee is not required] ... to search his mind for all thoughts relating to the [former] employer’s business and thereafter be precluded from employing [using] such thoughts when they are not trade secrets... An employer is only entitled to restrain a former

employee from disclosing and using confidential information which was developed as a result of the employer's initiative and investment and which the employee learned as a result of the employment relationship". [CTI Corp. v. Calhoon, 309 F. Supp. 762].

Another case stated:

"... to require a former employee, who has developed a new idea or concept following the termination of this employment and which is not based upon the [former] employer's secrets or confidential information, to turn over the fruits of this labors to his former employer constitutes, in the opinion of this Court, an unreasonable restraint of trade". [Armolite Lens Co. v. Cambell, 340 F. Supp 273 (1972)].

Therefore, the information and experience which Mr. Frumer obtained at Radguard, which was based upon general knowledge and methods for supervising and running R&D teams, is not a "trade secret". This is also true for methods of programming used at Radguard... Even the article submitted by Radguard's attorney, "Data Communications", supports our conclusion. This article compares companies in the VPN date protection field, describing what methods they use; these methods have become common knowledge and are not "trade secrets". Each companies' product is unique because of the way it combines these methods. Therefore, the "firewall" which Checkpoint has developed later became common knowledge. In this regard we bring an American judgment:

"... The Ninth Circuit has declared that ultimate goals and general concepts do not constitute trade secrets. General concepts cannot be claimed as an employer's trade secrets because they are 'general principles in the public domain and part of the intellectual equipment of technical employees.' Thus, concepts consisting of general principles such as programming principles do not qualify as trade secrets" [Winston Research Corp. v. Minnesota Mining & Mfg Co,].

Knowledge which is a "trade secret"

There are instances when knowledge in the hi-tech field, including that about specific programs, will be considered "trade secrets". This was described, as follows:

"An employee's unauthorized disclosure or use of his employer's application software has been held to constitute trade secrets

misappropriation under circumstances in which the governing employment contract included a provision concerning the employer's rights in software". [V.M. Gulbis, "Disclosure or Use of Computer Application Software as Misappropriation of Trade Secret"]

Regarding program applications and knowledge in worker's hands American courts have held what circumstances are considered "trade secrets" and we shall mention some of them:

"Former employees misappropriated trade secret of former employer, computer software developer, manner in which employer's generic utility programs interacted, which was key to its product's success, was not generally known outside of company, employer's combination of programs was not disclosed in its promotional literature... [the] former employees' created prototype data base manager program and other generic programs that operated in substantially same manner as comparable generic programs of former employer". [Gulbis, citing Integrated Cash Mgmt Inc v. Digital Transactions Inc. (1990), applying New York law.]

An indication that a computer program is a "trade secret" is that the confidentiality level is written on it... Further information which is considered a "trade secret", was described by Gulbis:

"... critical mathematical constants developed by the former employer, protectable methodology for implementing combination of concepts and ideas, manuals, program's source code, algorithms, modules and arrangement of elements...".

Another example mentioned by Gulbis:

"In action by corporation against its former president for misappropriation of trade secrets, based on defendant's alleged use of computer program that had been developed for plaintiff by defendant, a program designed for use in processing health care insurance claims electronically... plaintiff failed to prove that defendant 'used' secret information in developing competing program. Although information such as program's source code, algorithms and modules and its arrangement of elements, their sequence and order, which implemented idea of electronic submission of insurance claims to carriers for payment, were

sufficiently novel to constitute trade secret, evidence was clear that defendant's program ... was not copy of plaintiff's program". [Gulbis, citing Micro Consulting v. Zubeldia (1990), 813 F. Supp 1514.]

However, in order that this type of information shall be considered a trade secret the employer must inform the worker that it secret and, therefore, Gulbis has said:

"In order for information to be treated as confidential... the employee must be placed on notice as to the claimed status of the information...".

Products in the development stage as "trade secrets"

Development programs of hi-tech companies are part of their business plans. Hi-tech companies' decisions regarding which products to develop are of utmost importance to its' future and concern significant investments. Frumer was exposed to confidential information about the products which Radguard was developing. Such information is not common knowledge, cannot be easily obtained and is aimed at giving Radguard a business advantage over its' competitors. Therefore, based on the evidence before the court at this preliminary stage of the hearing, the only proven "trade secret" which Frumer has is Radguards development plans. Whether this knowledge prevents Frumer from working for a competitive company depends on the entire factual situation.

Nine months have passed from the time that Frumer left Radguard...However, the time necessary to develop hi-tech products is very short. It is a dynamic industry in which the development time of products is generally shorter than other industries, often about six months. Technology considered modern a year backward today. Our case illustrates the dynamic character of the hi-tech industry; within four years Checkpoint from a startup to a company employing 550 workers, with annual sales of \$200,000,000 and worth about seventeen billion dollars on the NASDEC... In light of the dynamic character of the hi-tech industry and based upon the facts presented at this stage of the hearing it can be assumed that during the nine months which have passed since Frumer left Radguard the products planned and developed while he was there have been completed. Furthermore, on the basis of Frumer's testimony and the evidence he appears to be a responsible and loyal person and there is no basis for Radguard's claim that he will reveal to Checkpoint confidential information.

Also, we cannot ignore the difference between the two companies: Checkpoint invented the firewall concept and is much bigger than

Radguard. Checkpoint's research and development programs are broader than those of Radguard. Therefore, we should not assume that Checkpoint needs information about Radguard's research and development plans. Moreover, Checkpoint's products are software based, while Radguard's R&D is in hardware. The companies chose different solutions to information protection. We, therefore, conclude that there is little chance that Radguard's R&D information known by Frumer nine months ago will be of value to Checkpoint.

Moreover, Radguard has not proven, at this preliminary stage of the hearing, that Frumer knows its' commercial secrets relating to the development of a specific new product, or reconstructed data, programs, formulas, algorithms, graphs, etc, which he can use at Checkpoint.

In light of the above reasons we conclude that as of today Frumer has no "trade secret" relating to Radguard's R&D program which justify granting an injunction.

The Finished Products -

Undoubtedly, Radguard's software and hardware which are registered patents are her property, despite there being public knowledge. Frumer's knowledge of this information is protected intellectual property. Relating to the protection of intellectual property Prof Glubus said:

"The protection of proprietary application software is an issue of economic importance to firms engaged in the development and use of such software in computer-assisted manufacturing processes and data processing. Apart from protection of such software as a trade secret, counsel may find it advisable to consider protection under patent or statutory copyright laws".

Radguard's "trade secrets" which are contained in its' products, such as computer chips and boards, are known to their purchasers. In effect, every purchaser has confidential knowledge and, theoretically, can copy it. Intellectual property laws protect Radguard from people copying their products and if Frumer does so he can be prosecuted. However, we shall not accept the presumption who works for a competitor intends to copy his former employer's products; there is no evidence that Frumer intends to do so.

Marketing, product faults, etc. –

As we have mentioned above, purchaser lists can be a trade secret, which justifies granting an injunction. However, Frumer did not work in marketing and there is no evidence that he took Radguard's customer list.

At this stage of the hearing there is no evidence to support Radguard's claim that Frumer has secret information regarding its' products vulnerable points and that such information is useful to Checkpoint. If Radguard's products have faults they are probably known to the public thru professional journals which compare the advantages and disadvantages of the VPN products on the market. It is fair and expected that companies inform consumers of their products faults, as a warning and to enable them to use the product. There is also no evidence that Checkpoint is interested in special knowledge about the vulnerable points of Radguard's products.

When can we assume that a worker will use “trade secrets” at his new workplace?

If it is proven that a worker has trade secrets of his former employer, there is still an important issue of when it can be assumed that he will use this information at his new work. A worker who knows a trade secret is not automatically prohibited from working for a competitor of his former employer. When the court is considering restricting a worker's freedom of occupation it shall give proper weight to the trade secrets he has only if there is a reasonable chance that he will use it and, thereby, cause actual damage to his former employer. This is an important issue because a skilled worker will seek employment in his occupation.

American courts have two approaches to this issue: **the first approach** – that the former employer must prove that there is a reasonable chance that the worker will use the trade secret at his new work. There is no assumption that he will do so. **The second approach** – there is an assumption that the worker will use his knowledge of a trade secret at his new work. This is called the “inevitable disclosure doctrine”. Adopting the much criticized latter approach will prevent many skilled workers from working in their occupation. [description of the American case Pepsico Inc. v. William Redmond and Quaker Oats Co, US Ct of Appeals, 7th Circuit (1995)].

My approach is that the court should examine carefully the factual situation of each case. There should not be an assumption that workers do not honor their legal obligations or their duty of loyalty to their former employers regarding trade secrets. In order to limit a person's freedom of occupation the former employer must submit evidence or point to circumstances which indicate a reasonable chance that the worker will use the trade secrets at his new work... The intentions of the worker and his new employer are important. Also, did the worker take documents from his former employer, did he do so “after hours” or when no one was present? Did he copy computer material? Did the new employer recruit the worker while he was working for the former employer in order to open a competing business? When the new employer has many departments his intentions

can sometimes be determined by whether he assigns the worker to a department in which the worker can use his trade secrets.

Will Frumer use his “trade secrets” at Checkpoint?

Frumer specifically undertook not to use or pass on in any way Radguard’s trade secrets. In this way Radguard protects its’ trade secrets and, if it can prove that Frumer violated his obligation, it can sue him. At this stage of the hearing there is no evidence that Frumer violated this obligation or that there is a reasonable chance that he will do so during his employment at Checkpoint... According to the documents submitted, Checkpoint did not search for one of Radguard’s former employees. Frumer did not turn to Checkpoint for work but was offered the position by a hi-tech manpower agency. Frumer did not resign from Radguard in order to work for Checkpoint, but because he was removed from his position as head of R&D and not offered another job. Further support for Frumer’s position is the letter of the manager of the hi-tech manpower agency which found him the position with Checkpoint. This letter was sent to the assistant director general of Checkpoint after Radguard objected to Frumer’s employment there. This letter reads as follows:

“At your request I shall relate to Mr. Frumer’s recruitment for work at Checkpoint. Checkpoint has searched for a manager of development teams in the computer communication field. Checkpoint never requested me to approach Dan Frumer or any other Radguard employee. Checkpoint did not request that I seek an expert in VPN. Mr. Dan Frumer approached our manpower recruitment firm in order to find him a challenging position. We offered him a number of possible positions, including Checkpoint. We also sent information on him to various companies. I note that there are few positions in Israel for managing development teams at the level which Checkpoint offered Frumer. In effect, Checkpoint’s offer was an unusual opportunity for someone on Frumer’s professional level and I knew of no other position on that level.... “

Furthermore, Frumer did not receive any special compensation from Radguard which justifies limiting his freedom to work. From the evidence presented Frumer’s salary at Radguard was that of a worker and not of an owner or founder...

Why Checkpoint?

Radguard’s position was that it did not object to Frumer’s working for any company in the world except Checkpoint. Indeed, a person with Frumer’s qualifications could find a position with another employer.

However, the manager of the manpower agency, quoted above, said that the work at Checkpoint was an unusual opportunity and that there were not many other similar positions in Israel. However, there is other evidence that Frumer received other work offers. From this my colleague [the minority opinion] learns that it is reasonable to limit Frumer's freedom of occupation by prohibiting him from working for one of Radguard's competitors. I reject this position. Frumer should be free to choose his place of work and determine his destiny; this is part of his right to self-fulfillment. As mentioned above, this right is granted him, unless there is a good reason to limit it. If Frumer thinks that the work at Checkpoint is more interesting and enables him to receive better work conditions, he is entitled to choose to work there. Moreover, in Israel there are few other companies in the information protection field and it is possible that Frumer wants to work in Israel rather than abroad. Also, in Israel there are few companies of Checkpoint's size working with information protection. The fact that Radguard and Checkpoint are competitors in the information protection field does not prevent their workers from transferring from one company to the other... It is natural that a worker will seek employment in his field of expertise; many people like to do work they have done and can obtain good working conditions by using their work qualifications. Therefore, it is not enough to claim that Frumer could find another position to justify limiting his freedom of occupation.

In conclusion –

... according to the facts before this court ... the temporary order issued by the Regional Court prohibiting Frumer from working for Checkpoint should not be continued, for the following reasons: Frumer was an expert in information protection prior to working for Radguard. During his work at Radguard Frumer increased his expertise and experience in this field, which is natural for a professional worker. Frumer's knowledge and experience is an integral part of his professional qualifications; these are Frumer's property, he can do with them as he wishes, even if there is a restraint of trade clause in his Labor contract...

... The only trade secret which Frumer has is Radguard's R&D plans, which are no longer a "secret" after nine months...

... Furthermore, Frumer and Checkpoint have acted in good faith and the facts of this case do not justify limiting his freedom of occupation.

I have the following comments regarding the minority opinion: [1] while only two weeks went by between the formal severing of employer-employee relations and Frumer's working at Checkpoint, three months passed between Frumer's resignation and stopping work at Radguard and his beginning to work at Checkpoint. [2] Indeed, contracts should be honored; however, public policy, freedom of occupation and Frumer's

right to self-fulfillment outweigh his contractual obligation. [3] My colleague does not point out a trade secret, other than the one mentioned in my opinion. There is also no evidence that Frumer used Radguard's trade secret while working for Checkpoint; [4] Frumer's ability to manage R&D teams is a much sought after expertise and it is reasonable that for this reason he was hired by Checkpoint.

.... We, therefore, accept the appeal, cancel the injunction prohibiting Frumer to work for Checkpoint.

ANNOTATION

This was the landmark case which changed the Israeli rule regarding freedom of occupation.