WIPO

Protecting Trade Secrets: Challenges in the Digital Environment

Guriqbal Singh Jaiya
guriqbal.jaiya@wipo.int
May 21, 2008
Genève, Switzerland

WIPO

Article 39 TRIPS Agreement

Natural and legal persons shall have the possibility of preventing information lawfully within their control from being disclosed to, acquired by, or used by others without their consent in a manner contrary to honest commercial practices so long as such information:

(a) Is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;

(b) has commercial value because it is secret; and

(c) has been subject to reasonable steps under the circumstances to keep it secret, by the person lawfully in control of the information.

WIPO

Three elements

Information is confidential

Relationship of confidence

Detriment from disclosure

WIPO

Trade Secrets

- Information
  - **Any information, ideas, data, test results (even negative test results), plans, intents**
- Confidential
  - **The information must be secret**
  - **Must use reasonable efforts to protect the secrets (protection/security measures)**
  - **Excluded: public information –**
    - **Submission of papers for publication – thesis**
    - **Marketing information**
    - **Regulatory filings**
    - **Laid open patent applications**
    - **Securities filings**

WIPO

Trade Secrets

Relationship of confidence

- **Relationship**
  - Need a relationship, does not work with the stranger
- **Obligation of confidence**
  - Obligation to maintain the information as confidential
  - May arise:
    - Expressly (e.g. contract, NDA, consulting term, etc.)
    - Implication (conduct – pre contractual negotiations)
    - By operation of law

Trade Secrets

- Detriment arising from the disclosure
- Generally easy to show detriment
  - Loss of control of the information
  - Loss of head start
  - Loss of reputation

Trade Secrets

- Remedies
  - Injunction
  - Damages
  - Tracing
  - Binding the innocent third party
- Defenses
  - Delay
  - Waiver
  - Estoppel
  - Bad conduct

Traditional Work Environment

Historically, most records were paper, generated locally, and controlled by just a few workers.

Nowadays, workers at all levels of a business - both within the office and offsite - create records anywhere in the world and at any time of the day.

WIPO

Work Environment Today 1

How We Work Today vs. 5 or 10 Years Ago:

Computers, e- mail, Internet, voice-mail are essential business tools.

The digital world brought new complexities and a broader definition of “data”, "record" or “document”. It also brought a dizzying array of media including e-mails, optical storage, voice recordings, mobile storage (laptop computers, thumb drives, smart phones, for example) and others.

WIPO

Work Environment Today 2

- The ongoing digital evolution creates a mix of both paper and electronic records.
- The number of unstructured digital records grows faster than structured data.
- Traditional records management policies and retention schedules neglect electronic formats and media.

WIPO

Work Environment Today 3

The definition of a "document" is expanding rapidly to include the many and varied files and fields of data that are now generated and stored electronically without ever producing a "hard" copy.

In addition to the final "document" there may be numerous drafts by numerous people.

E-mails provide their own special headache when attempting to determine the thread of an e-mail correspondence -- the recipients, the replies, the forwardings, the cc's, the bcc's, and the times of sending and openings of each e-mail.

WIPO

Work Environment Today 4

Individuals, through the use of various programs such as word processors, e-mail programs or spreadsheet programs, author some of these files. The programs themselves author others, as they keep track of the information input by humans. For example, an email generated in Microsoft Outlook has approximately 30 fields of information viewable by a user. The writer or reader of an e-mail generally pays attention to only a few of these fields: the To, From, Sent, Subject, and Message fields for example. Microsoft Outlook actually generates over 100 fields of data for every e-mail. The data stored in these fields that users rarely if ever view, often called "metadata" can sometimes be case-determinative in litigation.

Work Environment Today 5

Of course, other programs (most notoriously **Microsoft Word**), keeps track of a tremendous amount of **metadata** associated with a document, including changes made, by whom, when, and sometimes **unwise comments** left by drafters.

WIPO

What is Electronic Data? 1

- E-mails
- E-mail attachments
- Instant messages
- Word-processing files
- Spreadsheet files
- Database files
- Financial and accounting files
- Human resource and payroll files

WIPO

What is Electronic Data? 2

- Internet files
- Browser cookies
- Intranet files
- Graphics files
- Desktop faxes
- Other application files
- Voicemail
- Incompletely deleted files

Storage Problems

The storage problems associated with desktop faxes and voicemail files are indicative of the slippery slope on which we are standing as we try to apply older concepts of appropriate discovery to newly-developing categories of electronic data.

More and more companies and organizations are installing digital voicemail systems. In these systems, voicemails are saved as an electronic file on a hard drive comparable to any of the other types of files described above.

Where is electronic data? 1

Network servers; Desktop computers;
Laptop computers
Home computers ; Hard drives
Portable hard drives; Flash memory cards
Diskettes; CDs ; DVDs
Back-up tapes ;
Zip or other back-up drives
Offsite storage systems
PDAs
Cellular phones

WIPO

Challenges for Employers

1. Right to manage workplace.
2. Protect property and information of employer and its clients.
3. Protect employees.
4. Aid employer investigations.
5. Employee productivity.
6. Evidence.

WIPO

Employer Monitoring of Employee Communications

- **American Management Association 2005 Electronic Monitoring and Surveillance Survey.**
- See, http://www.amanet.org/research/
- Employer monitoring of employees' telephone calls, e-mail, internet connections, and/or computer files is about twice as much as reported in AMA's 1997 survey.

WIPO

Employer Monitoring of Employee Communications

(X) What is monitored?;(Y) Written policies inform employees?

i. Website connections/surfing 76% X; 89%Y

ii. E-mail 55% X; 34%Y

iii. Video for security 51%; 80%

iv. Video for performance 10%; 85%

v. Keystrokes, content, time 36%; 80%

vi. Computer files 50% X; 82% Y

vii. Phone time phone/numbers 51% ;78%

viii. Record calls (selected positions) 19%; 86%

ix. Voice-mail 15% X; 76% Y

Costs of Protection

- Constantly upgrading and monitoring of equipment and software
- Ongoing training of e-security staff and recruitment of new and more specialized employees
- Increase physical security, internal monitoring, and policies
- Difficulty in correlating e-security investment with overall company business

WIPO

Perspectives

- Privacy
- Security
- Secrecy/Confidentiality

WIPO

Knowledge Diffusion

- Trade Secrets (TS), knowingly or unknowingly, may be sent outside the enterprise to potential competitors. Once a TS is in the hands of others, it can be very difficult for an enterprise/company to prove that it owns the asset.
- A recent example in which knowledge diffusion nearly cost a company dearly is the thwarted attempt by a Coca-Cola employee to sell trade secrets to Coke's rival, Pepsi, in July 2006.

The Saving Grace!

Pressing the delete button does not mean it's gone forever:

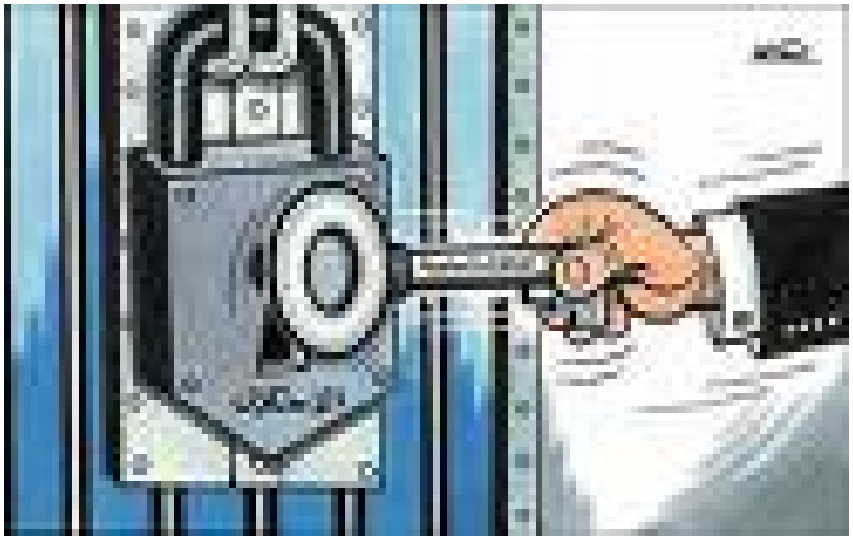
i. Electronic information and versions are stored in multiple places inside and outside company walls.

ii. Information thought to be deleted or lost can often be retrieved by experts.

WIPO

1

Putting in Place a Trade Secret Protection Program



WIPO

Importance of Authentic Business Records

July 5, 2006, Memo to all Coca-Cola Company Employees

"Sadly, today's arrests include an individual within our Company. While this breach of trust is difficult for all of us to accept, it underscores the responsibility we each have to be ***vigilant in protecting our trade secrets.*** *Information is the lifeblood of the Company. As the health of our enterprise continues to strengthen and the breadth of our innovation pipeline continues to grow, our ideas and our competitive data carry increasing interest to those outside our business. Accordingly, I have directed a thorough review of our* ***information protection policies, procedures and practices*** *to ensure that we continue to* ***rigorously safeguard our intellectual capital."***

– Neville Isdell, Chairman and CEO, Coca-Cola Company

Video surveillance

- Video surveillance cameras would not be so diligent in detecting trade secrets sent via email and secure file transfers to colluders inside and outside of Coke's network environs.
- In a legal dispute, Coke would be hard pressed to prove that they invented the secret formula first and that they even owned it outright, especially if Pepsi were to produce supporting business records that appeared legally credible and authentic.

Documents Discovery

- When companies are faced with IP challenges and risk losing valuable intellectual capital assets, all relevant electronic and paper documentation is discoverable and admissible in court.
- The US Federal Rules of Evidence allow for electronic records to be equally admissible as paper records in legal proceedings provided that (i) they are kept in the course of regularly conducted business activity; and (ii) the source of information or the method of preparation is trustworthy.

1. Identify “real” trade secrets and their value.

Evaluate confidential and proprietary information and answer two questions:

(1) What information, if taken by a competitor, could damage or destroy your business?

(2) How much money has or will the company spend to develop this information?

2. Develop a protection policy

Advantages of a written policy:

- **Clarity** (how to identify and protect)
- **How to reveal** (in-house or to outsiders)
- **Demonstrates commitment to protection** → important in litigation

Authenticity of Records

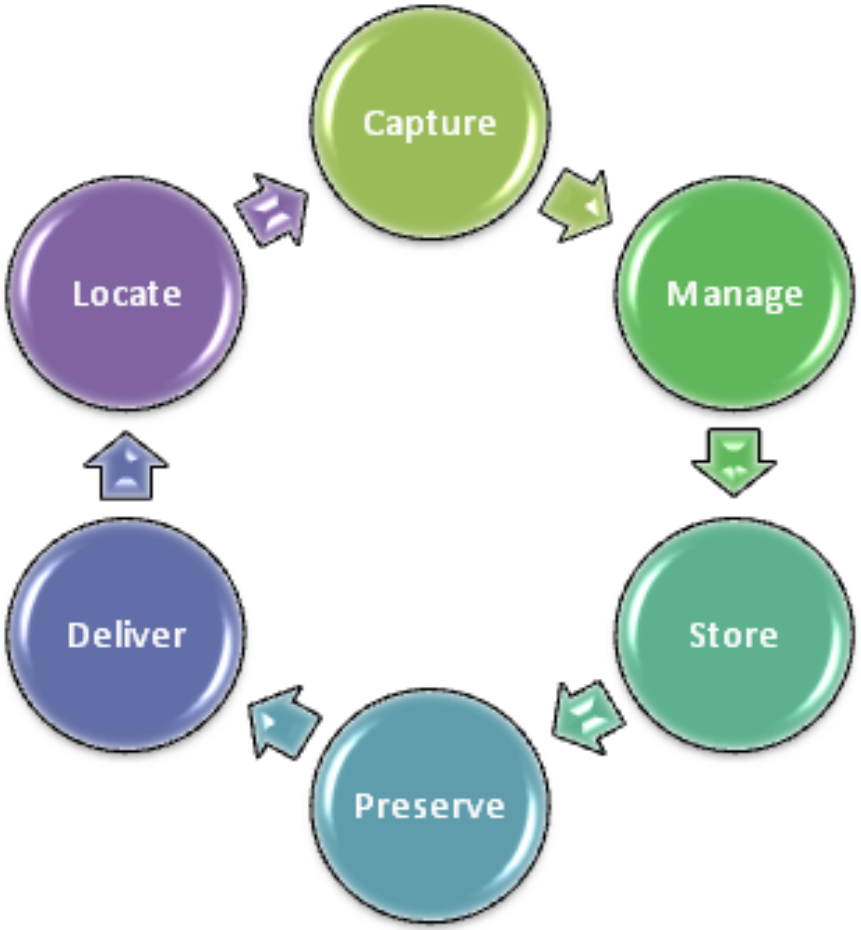
- Opposing counsel will not only challenge the authenticity and credibility of a company's records, but also, the trustworthiness of the people, processes and systems responsible for their safekeeping. Companies can present business records that credibly support their IP claims, but without irrefutable proof of their authenticity, they may be successfully challenged and eliminated as evidence. Such a challenge derives from the fact that unprotected electronic records can be easily altered or fabricated. Opposing counsel will attempt to show that employees of the company have motive and opportunity to manipulate records.

WIPO

Enterprise Content Management

WIPO

Enterprise Content Management



Risk Factors to Authentic Business Records

- The two primary factors inside the enterprise that drive the need for businesses to prove the authenticity of their business records are: **(i)** motive and **(ii)** opportunity.
- 1. **Motive.** More than 60 percent of all IT Security breaches are caused not by outside hackers, but by trusted insiders who have access to corporate intellectual property assets.

WIPO

Risk Factors to Authentic Business Records

- 2. **Opportunity.** With more than 90 percent of all business records now generated electronically, there are innumerable opportunities to tamper with electronic records. Forging or tampering with electronic records is easy to do and difficult to detect. Also, because electronic records can be generated in one department, managed in another, and archived in yet another, there are multiple points in the organization where manipulation can occur. This decentralized record management process poses a significant risk to senior executives, who when challenged must be able to prove the legal credibility and authenticity of these records throughout their chain-of-custody or risk losing their company's IP assets.

WIPO

Logs and Backing Up

- Under the U.S. government's Federal Rules of Evidence, your electronic records are as admissible in a court of law as your paper records.
- So keeping electronic logs and frequently backing up your electronic records is very important. This includes your file share, Web site, mail server, source code system, multimedia production system, financial database, customer records and customer relationship management database as well as any other electronic form of business material -- especially those which you consider to be trade secrets and IP of your organization.

WIPO

Practice litigation readiness

- You should ask yourself: "Can you withstand a data integrity challenge? Are you 'litigation ready'?" If you are, then you:
- Have the right people in place to manage your electronic record management systems;
- Have conceived, implemented and documented the right processes to ensure that your electronic records are classified, managed and preserved properly with the highest levels of security; and
- Have adopted the right technology and systems to capture, secure, manage and archive your electronic records.

WIPO

Education, Training, Monitoring

- **Educate and train:**
  - Clear communication and repetition
  - Copy of policy, intranet, periodic training & audit, etc.
  - Make known that disclosure of a TS may result in termination and/or legal action
- **Monitor compliance, prosecute violators**

3. Restrict access…

…to only those persons who **need to know** the information

→ In the computer system, limit each employee's access to data that is to be actually utilized or needed for a transaction

4. Mark documents

– Help employees recognize TS

→ **prevents inadvertent disclosure**

– Uniform system of marking documents

- **paper based**
- **electronic** (e.g., ‘confidential’ button on standard email screen; pop ups)

5. Physically isolate and protect

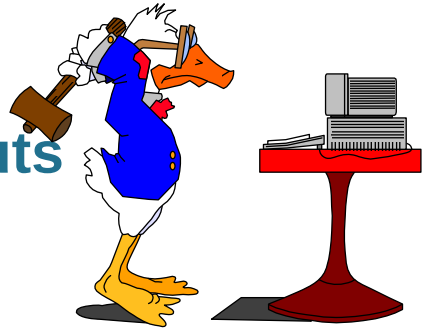
- **Separate locked depository**
- **Authorization**
- **Access control**
  - log of access: person, document reviewed
  - biometric palm readers
- **Surveillance of depository/company premises**
  - guards, video surveillance cameras
- **Shredding**
- **Monitoring/Oversight; audit trail**

6. Restrict access to facilities

- Log and visitor's pass
- Accompany visitor
- Sometimes NDA/CA
- Visible to anyone walking through a company's premises
  - type of machinery, layout, physical handling of work in progress, etc
- Overheard conversations
- Documents left in plain view
- Unattended waste baskets

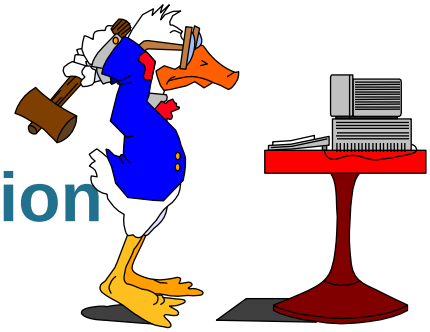
7. Maintain computer secrecy

- In defining “IT” or “Computer system”, consider:
- software, e.g. operating systems, firmware, middleware, interfaces, websites, applets, macros, development tools, formulae, development tools
- computer languages and format (e.g. object and source code)
- data, databases, files
- hardware, servers, switches, routers, printers, peripheral equipment, cabling, mask works, chips, equipment
- websites, domain names, website content
- architecture, structure, display screens, layouts
- networks, telecommunications, circuits



7. Maintain computer secrecy

- **Secure online transactions, intranet, website**
- **Password; access control**
- **Mark confidential or secret** (legend pop, or before and after sensitive information)
- **Physically isolate and lock: computer tapes, discs, other storage media**
- **No external drives or USB ports**
- **Monitor remote access to servers**
- **Firewalls; anti-virus software; encryption**



8. Measures for employees

1. New employees

- Brief on protection expectations early
- Obligations towards former employer!
- Assign all rights to inventions developed in the course of employment
- NDA/CA
- Non-compete provision
- Covenants prohibiting solicitation of customers, clients or other employees.

Nondisclosure Agreements

- Need to be careful - discount informality of the agreement
- Key terms:
- Standard of care is required for the obligation of confidence?
  - strictly confidential
  - same efforts as for own confidential information
  - "all" efforts
- How is "Confidential Information" defined?
  - include oral disclosure?
  - limit to written disclosure?
  - limit oral disclosure to that recorded in a specific time frame?
  - disclosure of confidential information
- Review restriction on use of the confidential information
  - How broad or narrow is the permitted use?

WIPO

Non-Competition Clauses (covenants not to compete) in Emplyment Contracts

After employee leaves prior employer:

- May he work for competitor?
- May he work in related job?
- May he open a competing business?
- Is covenant not to compete enforceable?

8. Measures for employees

1. New employees

- **Non-Solicitation of Employees**. Prohibition on soliciting or pirating employees and consultants away from Company.
- **Non-Solicitation of Clients**. For a period after employment ends, prohibition on soliciting clients or customers away from Company.

2. Current employees

- **Prevent inadvertent disclosure** (ignorance)
- **Train, educate and monitor**
- **NDA for particular task**

3. Departing employees

- **Limit access to data (Escort to desk)**
- **Exit interview**
- **Letter to new employer**
- **Treat fairly & compensate reasonably for patent work**
- **Doctrine of Inevitable Disclosure**
- **Springboard Doctrine**

3. Departing employees

- **Simply remove and securely store the hard drive of key employees before reassigning their computers.**
- **This step, which is essentially pre-litigation preservation, is cheap insurance should it become evident months down the road that an ex-employee has successfully launched a competing business using the company's confidential information.**

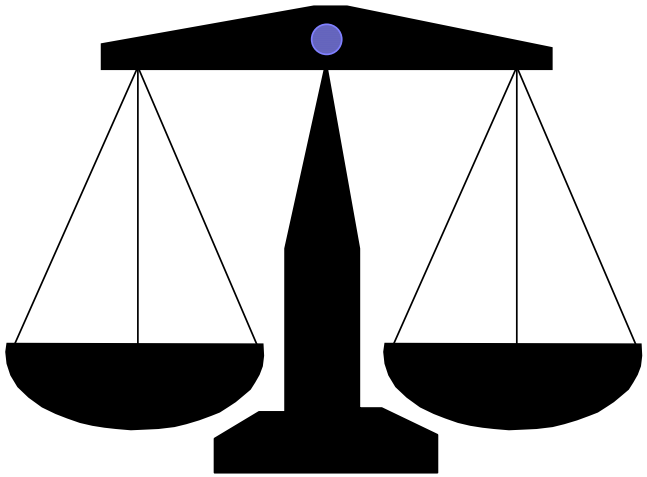
WIPO

Freedom of trade & commerce

Freedom to work

Autonomy of individual

Right to property
- IP, TS
- investment



Right to property:
- knowledge
- experience

Freedom of contracts

Innovation and Creativity

Prohibition of unfair competition

- **Some jurisdictions: NC covenants prohibited or are binding only if deemed to be ‘reasonable’**
  - limited in time; limited in area
  - limited in type of industry
  - special compensation to be paid to employee for his obligation not to compete
- **Covenants prohibiting solicitation of customers**
- **Covenants prohibiting “employee raiding”**
- **Covenants limiting employee's preparations for a competing business while still employed. Similar to employee's fiduciary duty of loyalty to employer.**

9. Measures for third parties

- Sharing for exploitation

- Consultants, financial advisors, computer programmers, website host, designers, subcontractors, joint ventures, etc.

- **Confidentiality agreement, NDA**
- **Limit access on need-to-know basis**

Challenges

➔Certain aspects of business/products cannot be maintained as a trade secret

- information or technology that must be disclosed to the public in order to market the product
- information or technology which is part of a product sold to the public and can be reverse-engineered
- mass-marketed technology or products
- where competition is so intense, that very likely to be independently developed by others within short time
- rapid personnel movement amongst competitors

WIPO

Response

➔ **Alternative or additional protection for TS**:

- **make reverse engineering difficult (compiled code)**
- **technological protection measures**
- **patents**
- **copyright protection**
- **Trademarks (Coke)**