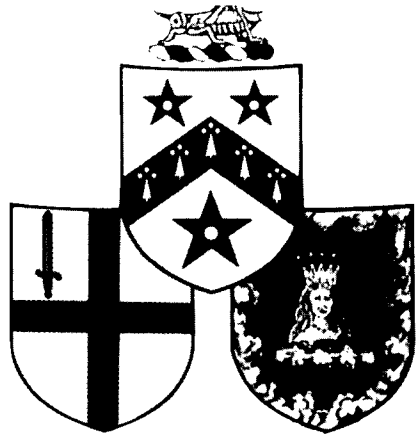
G R E S H A M

C O L L E G E



WORLD CYBERSPACE LAW

Lecture 4

CATEGORY OF CASES

by

PROFESSOR GERALD WAKEFIELD
Gresham Professor of Law

2 February 2000

CATEGORISATION OF LEGAL DISPUTES ON THE INTERNET

I think the best way to categorise the cases starting to be fought as a result of issues on the Internet would be to look at the various cases from different jurisdictions to give you a broad introduction. We can look to categorise under various headings however I have chosen to use the conventional legal terminology to differentiate the main categories that I described in an earlier lecture on encryption regulations. I proffered eleven distinct components of cyberspace law as:

- jurisdiction and related issues
- freedom of expression
- intellectual property
- privacy protection
- safety concerns
- equal access
- electronic commerce
- data protection
- Choice of Law
- Security
- Contract at a distance

In this lecture, let me start with one that could affect all of us because of the nature of the Internet and the ease with which anyone may publish information.

Defamation may be considered as a subset of freedom of expression

The Internet has exponentially amplified the potential sources of claims arising from internationally broadcast false statements and defamation. Cross-border defamation cases exemplify that alien defendants may successfully avail themselves of motions to dismiss for lack of personal jurisdiction as a first line defence by challenging due process. With the advent of new technology, people who were previously unable to publish due to cost barriers may now instantaneously broadcast text and graphics point to multi-point around the world via the Internet. This media, like others, may be used to publicise **misinformation**. Sending unsolicited junk mail embedded in electronic messages, for example, is a discouraged practice that is colloquially known as "**Spamming**".

For defamation cases, the decentralised nature and severity of injury to reputation are not entirely new issues, but new points may arise in cyberspace.

If we look at some recent cases in France we will see how the French jurisdiction deals with cases on defamation. The first case we shall look at is:

AXA Conseil IARD et AXA Conseil Vie v M. Christophe Sapet (Chairman of Infonie) Tribunal d'Instance de Puteaux, 28 September 1999. In this case a district court in France has decided who may be liable for defamation on the Internet.

Facts

Finding that a private web page hosted by Infonie contained slanderous allegations against them, two insurance companies sued the author (who was at the time an employee of the insurance companies), the ISP Chairman and the ISP for defamation.

The court held the author liable since he was held to have publicly damaged the companies' reputation. The court stressed in particular the fact that the damaging allegations had been made available to the public – which is one of the legal requirements for defamation – since they were contained on a private web page indexed on an internet search engine. It should be noted that the court observed that this would not have been the case had the allegations been contained in a private email message.

The plaintiffs further claimed that, pursuant to the French act on Broadcasting of 1986, the ISP Chairman was liable as the editor.

This claim was rejected by the court on the ground that, according to the act, **an editor may only be liable if the slander has been materially fixed prior to the publishing**, which is not the case on the Internet. The ISP indeed provides the technical means to make the information available but does not itself provide the information to the public. In other terms, the ISP does not have any control in real time over the information and cannot be regarded as an editor pursuant to the 1986 act.

As a result, all the claims were rejected by the court, since the plaintiffs were requesting the conviction of the ISP Chairman as the principal author of the defamation and of the ex-employee as a mere accomplice. Since the ISP Chairman was not liable, the employee could not be an accomplice, although the court would have been prepared to convict him as the principal author of the defamation.

However, the court insisted on the fact that the author of the slander was an identified natural person. In this respect, it is not clear whether the solution would have been the same had the author remained unknown. In such a case, pursuant to the 1986 act, it seemed that the court would have judged the ISP liable as producer of the damaging message.

It is interesting to compare this case with another French case determined by the Tribunal de Grande Instance de Nanterre, on the 8th December 1999. This case is **Lynda Lacoste v Multimania Company.**

For the second time in two years, a French court held an ISP liable for having permitted to be displayed on web pages they were hosting, nude photos of a French model who did not consent to such a display.

Facts

The four summoned ISPs were mainly relied on the provisions of the proposed **EU Directive on electronic commerce**, according to which hosting service providers may only be held liable if they are authors of the infringing act or if they did not respond after having been informed of such an act.

In addition, the ISPs argued that they were not bound to control and watch the pages they were hosting. Finally, one of the ISPs requested that judgement be postponed so long as the author of the web pages complained of had not been identified.

Court Decision

The Nanterre court dismissed their arguments and held all of them liable.

First, the application to postpone judgement was dismissed on the grounds that the ISP requesting it originated of the difficulty of identifying the author of the web pages, since it did not require identification at the time of the subscription. The ISP thus enabled the author to act anonymously with a guarantee of complete irresponsibility. According to this obiter dictum, an ISP should required identification elements which would, controversially, prevent Internet users from remaining anonymous – This obiter raises several privacy issues, and I refer you to the lecture on Privacy and the UK data protection Act.

Secondly, considering that, unlike an Internet access provider, the activity of an Internet hosting service provider goes beyond the mere conduit of information, and consists in the

communication of ideas, opinions, information, services, **the court decided that ISPs are bound by general obligation of care**. Consequently, an ISP must implement the necessary and appropriate means of information, control and action.

As regards the obligation to inform, the court considered that **an ISP must clearly inform its clients at the time of subscription of their obligation not to infringe third party's rights, and in particular personality rights**

Regarding the control obligation, the court laid down the principal that **an ISP does not have a general obligation to meticulously and deeply control the content of the web pages it hosts**.

However, **an ISP must adopt the reasonable measures that a professional would implement to avoid pages whose illicit nature is obvious; for instance, search engines may be used for this purpose if launched on certain key words (nakedness, beauty, celebrity, etc.).**

Regarding the obligation to act, the court considered that **ISPs discharged their obligation by immediately closing a litigious web site, although they do not have the appropriate means to ensure that the web site is not re-opened afterwards**.

Finally, the ISPs were ordered to pay Mrs Lacoste various amounts ranging from FFr. 20,000 to 100,000, depending upon the nature of the web site (pornographic or not) and upon the degree of care, one ISP was judged as having fulfilled his information and action obligations.

Two ISPs were ordered to publish on the home page of each of the hosted web sites and during 30 seconds each time and for 10 days the following message: "pursuant to a judgement held on 8th December 1999, France Cyber Media and SPPI were ordered to pay damaged for having hosted web sites infringing personality rights. The companies have the possibility of suing the Internet users who are the authors of the litigious web sites in order to obtain payment of the sums paid."

The ISPs were also ordered to adopt the appropriate search measures to find and eliminate the web pages containing photographs of the plaintiff, subject to a penalty of FFr. 10,000 per infringement.

This particularly severe judgement should give rise to abundant comment since it apparently runs contrary to the current terms of the proposed EU Directive.

I would like to look now at a recent US decision which has international ramifications. The case is **the Federal Trade Commission v Pereira**. This was in the US District Court of the Eastern District of Virginia, 20th September 1999.

Facts

On 20th September, 1999, the US Federal Trade Commission (FTC) obtained a preliminary injunction, and is seeking a permanent injunction, against an Australian operator of sexually-explicit web sites and a Portuguese computer hacker for their elaborate scheme in which they drew unsuspecting Internet users to their sexually explicit web sites. The defendants had used technological tricks to commandeer over 25 million web sites in order to divert unsuspecting search engine users, including children, to the defendants' sexually explicit sites, in a process known as **"Page-jacking"**, and then locked users into a loop of continuously reappearing sexually-explicit web pages, in a process known as **"Mouse-trapping"**. As part of the preliminary injunction, all parties hosting the defendants' web sites were ordered to block access to defendants' sites, and Network Solutions Inc, the domain name register, was ordered to suspend the domain name registrations for defendants' offensive sites, thereby effectively shutting them down.

Page-Jacking/Mouse-trapping

The defendants' made use of search engines and **meta-tags** to page-jack approximately 25 million web pages from diverse unrelated sources, including commercial, educational, and entertainment sites. Search engines are the programs which search Internet contents for key words and which provide lists of Internet pages containing the key words. Meta-tags are words and/or phrases which are part of the hidden source code of the web page, and which tell search engines about the page's content for indexing.

As part of the page-jacking process, the defendants copied web pages, including the meta-tags, so that defendants' pages would appear in search engine results for subjects searched. For example, users of search engines to located sites on Oklahoma Tornados, children's songs, or pie recipes would find the defendants' sites, along with legitimate sites, included in the search engine results. Furthermore, the description for defendants' sites would read exactly the same as the description for legitimate sites.

Users who clicked on the false search engine results were automatically diverted by a Java script command the defendants had added to the source code, to defendants' sexually explicit web sites. Users were then mouse-trapped into a continuous loop of sexually explicit sites because the defendants also manipulated the functioning of the users' Internet browser by immobilising the users' "back" and "forward" buttons. When users attempted to leave defendants' sites, they were instead directed to additional adult sites. Users had little recourse but to turn off their computers to get out of the loop.

Court decision

Section 5 (a) of the Federal Trade Commission Act

Brought under Section 5(a) of the Federal Trade Commission Act, which prohibits unfair or deceptive acts or practices in/or affecting commerce, the FTC maintained that the defendants had committed both unfair acts and deceptive acts. The defendants have committed deceptive acts by misrepresenting the real identity of their web sites in search engines results and they have committed unfair acts by page-jacking the web sites and mouse-trapping unsuspecting users. The FTC's examples of the substantial injury to users from unfair practices include reports that a child searching for information about Kosovo was trapped in one of their sexually explicit web sites until his father intervened, and also that an adult user was subjected to possible dismissal by his employer because he had been forced to the offending sites during a workplace search, thereby violating the employer's policy against accessing adult sites.

The FTC presumes that the defendants ran the scheme in order to maximise the revenues they could make by directing users to other adult web sites; and/or by drawing heavy traffic to their sites thereby enabling them to charge top prices for the banner ads displayed on their sites, practices which are prevalent amongst adult sites.

Jurisdiction over the Defendants

Although all defendants reside outside the US, the FTC asserts that the court has jurisdiction over them because **the defendants' many US contacts constitute a minimum of contacts sufficient to satisfy the US constitutions due process requirements. US case law holds that in actions brought under Federal statues like the FTC act, a court may exercise jurisdiction over foreign defendants where they have minimum contacts with the US.**

Further, where the defendant has **"purposefully availed himself of the privilege of conducting activities in the forum", and injuries arise out of these activities, and the**

exercise of jurisdiction is reasonable, a court may exercise jurisdiction over a non-resident defendant. With regard to cases involving Internet activity, US courts have generally found that defendants using the Internet actively to construct and solicit business in a particular jurisdiction have the requisite minimum contact with that jurisdiction.

The FTC maintains that the US District Court of Eastern District of Virginia has jurisdiction because the defendants have "**purposefully availed**" themselves of the forum and because the FTC's claim against the defendants arises out of their many contacts with the US and particularly in the district.

The defendants had registered many domain names with domain name register Network Solutions Inc. and as part of the registration agreement they consented to jurisdiction in the eastern district of Victoria to settle domain name disputes. Furthermore, the defendants had page-checked web sites from all over the US; they had "manipulated" search engines on Altavista, the popular US search engine, and they had "victimised a multitude of US consumers for their own commercial gain." The FTC further states that the court's exercise of jurisdiction is "**reasonable**" based on the defendants' many contacts and based on a compelling state interest in enforcing consumer protection law.

Ozú v Ozú

The facts

in March 1996, a Spanish company under the name Advernet launched a search engine called Ozú with the business drive to become a reference tool for Spanish-speaking Internet users in a market controlled by entities operating search engines running in English. The company explored its potential by including the search engine in its web page accessed through the domain name *advernet.es*. Recognising its rapid success, the company decided to market the search engine separately and proceeded to obtain the domain name *ozu.com* through an American entity called Admazing Inc. Subsequently, in November 1996, Advernet obtained registration with the Spanish Patent and Trademark Office (SPTO) of the trademark Ozú for its search engine.

A shareholder in Admazing, programmer of the software on which Ozú was running and the commercial partner of Advernet, immediately changed the access keys of the search engine, so gaining control of it and thus of the domain name *ozu.com*. Deprived of its search engine, Advernet went on to created a new one under *ozu.es* in January 1997, so that there were two identical tools operating on the Web under the same name.

Advernet filed a legal action against its former partner and his Spanish company Ozucom (through which web site the search engine was also commercialised) on grounds of trademark infringement and trademark dilution, requesting an immediate injunction against the infringing acts and the use of the domains *ozu.com* and *ozucom.es*, demanding Ozucom's corporate name be changed and claiming compensation for damages.

The defendant counter-claimed, requesting the dismissal of Advernet's action and the enforcement of his intellectual property rights over the computer program on which Ozú runs, the recognition that the registration of the plaintiff's trademark infringed his rights, the immediate injunction against the use of the term Ozú to refer to an Internet search engine, and compensation for damages.

The Judgement

The Court reasoned that trademarks, as distinctive signs of companies in the commercial arena and fundamental instruments of consumer protection, are to be regarded as one of the relevant intangible assets in today's world. Accordingly, trademark protection should be recognised as belonging to the individual or company providing its ownership vis-à-vis the user of other signs which lead to confusion on the part of consumers. Ozu, being used by both parties, was only registered in the name of the plaintiff.

The Court reached the conclusion that the creator and owner of the search engine Ozú was Advernet, notwithstanding the programming help of Admazing. Further, the fees for the obtaining of the domain name ozu.com were paid by one of Advernet's shareholders and the bulk of the work to launch the search engine had been carried out by the company. The Court, then, decided for Advernet, granting an injunction against acts infringing the trademark, banning the use of the domains *ozu.com* and *ozucom.es*, mandating a change of the defendant's corporate name and awarding damages to be determined at a future date.

An appeal has been lodged against the court's ruling.

Trademarks on the Internet

This judgement demonstrates the importance of adequate protection of intellectual property rights in Internet activities and the key role their proper management will have for companies acting on-line.

The Ozú decision hinges upon a phenomenon which has caused considerable disruption in the traditional approach to this particular body of law, i.e. the impact the Internet has had on trademark law. Traditionally, trademarks have been the sole intangible means companies had to convey to the public their products or services. However, with the advent of the Internet the domain name has become part of the intellectual net worth of companies in a significantly qualified way, i.e., whereas the trademark is invariably linked to a certain product or service (the so-called speciality criterion of the trademark), because of the structure of the Internet a domain name is not to be necessarily linked to a product or service. For example, in the off-line world, two companies dealing respectively in insurance products and garments may share the same trademark because the mark clearly identifies a service and a product which definitely have different scopes and areas of activity. A domain name, on the other hand, is by definition unique and thus companies with the same name of trademark have had trouble accessing the Net because other companies with an identical name or trademark for different products or services have gone on-line previously.

Likewise, companies with a legitimate interest in a name or trademark have been deprived of their right to act on-line under it due to the existence of parties who have taken advantage of the first-come-first-served rule governing domain name registration in a wrongful act of cyber-squatting. Enterprises should therefore be diligent in ensuring trademark registration, which may eventually provide some relief, significantly in countries like Spain where protection is granted by registration and mere use furnishes almost no rights in respect of it.

Moreover, trademarks may be infringed in a number of new ways, i.e. framing and meta-tag practices. In a recent search through a search engine on the EPO (European Patent Office), six web sites of sexual content and fifteen sites unrelated to patents or EPO activities were found. Whereas any defence to these practices is difficult with a trademark, without one it may be impossible to mount such defence.

Companies are therefore strongly recommended to effect adequate protection of their intellectual property rights by effectively covering all grounds of intangible net worth available to them, including trademarks and domain names. There are numerous problems about their co-existing due to the obvious differences of the scenarios in which they operate. Although the solution to the problems their joint existence gives rise to is certainly difficult as they relate to different layers of reality, it would make sense to attempt to tackle these problems through organisations like WIPO (the World Intellectual Property Organization) which have responsibilities in respect of trademarks in the off-line world and have initiated studies on

conflicts between trademarks and domain names; see the WIPO Report on *Internet Domain Names Process* dated 30 April 1999 (hereinafter, WIPO Report, see http://www.wipo.int).

In this profound study aimed at outlining practices designed to minimise conflicts deriving from domain name registrations, WIPO recommends the obtaining of a domain name by means of a domain name contract between the registration authority and the domain name applicant where certain parameters are set out. The main items to be reflected in the contract are:

- (i) the identification of the applicant;
- (ii) the agreement of the applicant to be subject to an arbitration procedure in case of disputes which related to intellectual property matters arising out of domain name registration;
- (iii) the representation that to the applicant's knowledge and belief neither the registration or the manner in which a domain name is directly or indirectly used infringes any intellectual property rights of third parties; and
- (iv) the agreement of the applicant to submit itself to certain courts (the jurisdiction of the courts of the country of domicile of the domain name applicant and the country where the registrar is located).

The WIPO Report, drawing heavily on the experience of customers, enterprises, official bodies and experts alike, falls short of endorsing a potentially conflicting trademarks search by the registration authority prior to the granting of domain names, but it does encourage domain name applicants voluntarily to carry out such a search themselves. The Report also recommends the enforcement of an automatic process of verification of the applicant's data, and suggests that inaccurate information in such data (or failure to update information) should be grounds for the cancellation of the domain name.

In cases where the rights of owners of identical trademarks in different areas of activity conflict, the WIPO Report proposes the implementation of a common portal as a means of avoiding the disputes among those owners. Such a portal should provide a common entrance to a list of names using a common element and thereafter arrange links to the various addresses where each owner should be able to distinguish itself from the other(s). Although it is recognised that this solution may prove insufficient to owners of trademarks who clearly wish to preserve their unique identity and do not wish to share their rights with another, owners' good faith is invoked to consider such an alternative.

It goes without saying that underlying today's disputes a significant economic problem looms, due to the fact that enterprises are well know (and increasingly so) by their intangibles. Adequate protection of its intangible capital is a must for any company acting in our global economy , in view of the growing impact of modern economic practices which are heavily reliant on such intangibles. In fact, domain names, as trademarks, are an additional part of the intellectual property of enterprises and deserve all due respect and careful management within their commercial strategy, as the case law described demonstrates.

Contractual Implications on Internet Shopping

Facts

Some two to three months ago, catalogue chain store Argos learned an expensive lesson about e-commerce retailing following their web advert advertising televisions for sale at £3 instead of £300.

The Argos web site was inundated with bargain hunters placing orders for the cut-price televisions including one customer who apparently ordered 1700 of them. Once it realised the mistake the company announced that it did not intend to 'accept' any of the orders placed. Unfortunately one of the potential customers turned out to work for a City law firm and the firm has decided to back her in a test case against Argos.

To analyse the legal problem, it is necessary to go back to the basics of contract law. The typical classical contract is 'a bilateral executory agreement. It consists of an exchange of promises; the exchange is deliberately carried through by the process of offer and acceptance, with the intention of creating a binding deal. When the offer is accepted, the agreement is consummated, and a contract comes into existence before anything is actually done by the parties. No performance is required...The contract is binding because the parties intended to be bound...When the contract is made, it binds each party to performance or, in default, to a liability to pay damages in lieu. Prima facie these damages represent the value of the innocent party's 'disappointed expectations'.

The first question to consider is whether Argos made an offer to sell when they advertised their goods for sale at £3. The web page specifically stated that all orders were to be subject to e-mail confirmation. If a web page is viewed by the courts as a virtual shop front or on a par with a circular or hard copy advert the answer is probably no. An offer implies a final readiness to undertake an obligation, an intention to implement a promise, which the proviso about e-mail confirmation probably give the lie to. In ***Pharmaceutical Society of Great***

***Britain v Boots Cash Chemists (Southern) Ltd [1952]* 2 QB 75** it was held that when a customer helps himself to an item, places it in a basket and takes it to a till, this does not constitute acceptance to buy but rather an offer to buy because the shop could simply refuse to sell the item. A comparison was made with a customer browsing in a bookshop and wanting to buy a particular book, which had already been promised to another customer. The court said that the shopkeeper would be perfectly within his rights in refusing to sell it.

That may get Argos off the hook as far as the customers to whom they had not sent e-mail confirmations. However, the legal employee is said to have received an e-mail. This implies some step must have been taken by the customer (for example submitting her credit card details and hitting the 'place order' button, which, continuing the analysis of the contractual process, would probably be categorised as ***offer to buy.*** The next step in the process to contract is *acceptance,* which must be communicated to the offeror. If the 'postal' analogy is drawn, a bald confirmation by e-mail of a placed order might be treated as an acceptance by the retailer as soon as it is sent. On the other hand it could be argued that e-mail communications are analogous with telex transmission that the acceptance is not effective to bind the parties to a contract until it has been received. In reaching this conclusion about telexes *in* ***Entores Ltd v Mile Far East Corporation [1955] 2 All ER 493, 498*** the Court of Appeal emphasised the instantaneous nature of the transmission: 'though the despatch and receipt of a message is not completely instantaneous, the parties are to all intents and purposes in each other's presence just as if they were in telephonic communication, and I can see no reason for departing from the general rule that there is no binding contract until notice of the acceptance was received by the offeror'. There are arguments on both sides, which have not yet been resolved by the courts. As with posting a letter, an e-mail is put into the hands of an independent carrier in the form of the ISP and the sender cannot know when it will be received. Like a telex, however, an e-mail can be virtually instantaneous and telephonic conversations are possible over the internet.

A sensible e-commerce retailer can do a lot to protect itself from many hazards by the careful design of the web page in what has been dubbed a 'web-wrap' or 'click-wrap' contract. The buyer should be taken through a series of pages, giving full details of the product and the supplier's terms before finally asking the buyer whether those terms are accepted. However, it is difficult to conceive of a reasonable clause, which would allow a retailer to supply goods at a different price to the one advertised Moreover if the retailer gives a misleading price indication it will be an offence under s. 20 of the Consumer Protection Act 987 (for more detail see also the Consumer Protection Code of Practice for Traders on Price Indications) Approval Order 1988 SI1988/2078) which apply to mail order and e-commerce transactions.

However, the Act specifically provides that if a mistake is made it will be a defence provided the person (including a corporate person) can show that he took all reasonable precautions and exercised all due diligence to avoid such an act of omission by himself or any person under his control. For example, if the mistake was the result of a typing error which was accidentally not picked up at the proof reading stage a company is likely to escape conviction.

However in the case of Argos, clearly they did not mean what they seem to have said. Can they argue that their mistake in not saying what they meant was such an obvious mistake as to invalidate the contract? Where the fact that one party has made a mistake as to the terms of the contract and the other party knows that the mistake has been made and seeks to take advantage of it, the court will come to the rescue of the maker of the mistake. However, in this context it is not enough to show that it ought to have been objectively obvious that a mistake had been made, it must have been actually known: ***The Nai Genova [1984] 1 Lloyd's Rep 353.*** It may be possible to prove knowledge by inference (for example, where the parties had traded before on similar terms as in ***Hartog v Colin and Shields [1939] 3 All ER 566)*** but this seems unlikely to apply in the case of a one-off consumer sale.

Looking at the contractual issues it seems more likely that Argos will not be found liable except where they actually confirmed their acceptance of the order. They could have committed a criminal offence unless they can show mistake and 'due diligence'. However, they will be at their weakest having to rely on mistake as a defence in civil proceedings.

Safeguards in legislation relating to search and seizure conditions particularly relating to human rights

I would draw your attention to the new Communications Bill drafted by the DTI. Although they have amended the original bill, there still is room for improvement.

From this point of view, it is interesting to analyse the one case in which the court has held that safeguards provided were sufficient. In that German case, Class v Germany 2 EHRR 214, decided in 1978, the court held that the relevant legislation provided for:

1. Surveillance could be ordered only on written application giving reasons, and such an application could be made only by the head or his substitute, of certain services;

2. The decision thereon must be taken by a Federal Minister empowered for the purpose by the Chancellor or, where appropriate, by the Supreme Land Authority;

3. The competent Minister in practice and except in urgent cases sought that prior consent of the Parliamentary Commission charged with supervising the law;

4. The measures in question remained in force for a maximum of three months and may be renewed only on fresh application;

5. The measures were immediately discontinued once the required condition had ceased to exist or the measures themselves were no longer necessary;

6. Knowledge and documents thereby obtained could not be used for other ends;

7. Documents had to be destroyed as soon as they were no longer needed to achieve the required purpose;

8. Initial control of the implementation was carried out by an official qualified for judicial office. This official examined the information obtained before transmitting to the competent services such information as may be used in accordance with the act and is relevant to the purpose of the measure;

9. He destroyed any other intelligence that may have been gathered;

10. While recourse to the courts in respect of the ordering and implementation of measure of surveillance was excluded, subsequent control or review was provided by two bodies appointed by the Parliament, namely the Parliamentary Board and the G10 Commission;

11. The competent Minister had to report at least once every six months to the Parliamentary Board consisting of five members of Parliament;

12. In addition, once a month the Minister had to provide the G10 Commission with an account of the measures he has ordered;

13. The G10 Commission decided, ex officio or an application by a person believing himself to be under surveillance, on both the legality of and the necessity for the measures in question; if it declared any measures to be illegal or unnecessary the Minister had to

terminate them immediately. The Commission members were appointed for the current term by the Parliament;

14. The person concerned was notified, after the measures had been discontinued, that he had been subject to surveillance, several legal remedies against the interference with his rights became available to him;

    i) an action for the declaration i.e. a review by the administrative court of the legality of the application to him of the surveillance measures and its conformity with the law;

    ii) an action for damages in the civil court if he had been prejudiced;

    iii) an action for the destruction of, or if appropriate, restitution of the documents; and

    iv) as a last resort, apply to the Federal Constitutional court for ruling as to whether there had been a breach of the basic law.

The safeguards provided in the draft Bill come nowhere near those approved by the court. No provision is made for independent judicial control. This is left to the highest ranking official in the respective law enforcement agency or the Secretary of State in relation to MI5 and MI6. Furthermore, the Commissioner and Tribunal envisaged under the bill will only be empowered to review those parts of the operation of the scheme which requires the permission of the Secretary of State, this leaves the vast majority of persons "with the appropriate permission" outside their jurisdiction.

GRESHAM COLLEGE

Policy & Objectives

An independently funded educational institution, Gresham College exists

- to continue the free public lectures which have been given for 400 years, and to reinterpret the 'new learning' of Sir Thomas Gresham's day in contemporary terms;

- to engage in study, teaching and research, particularly in those disciplines represented by the Gresham Professors;

- to foster academic consideration of contemporary problems;

- to challenge those who live or work in the City of London to engage in intellectual debate on those subjects in which the City has a proper concern; and to provide a window on the City for learned societies, both national and international.

Gresham College, Barnard's Inn Hall, Holborn, London EC1N 2HH
Tel: 020 7831 0575 Fax: 020 7831 5208
e-mail: enquiries@gresham.ac.uk