18th BILETA Conference:*Controlling Information in the Online Environment*

April, 2003
QMW, London

ICANN's Role in Controlling Information on the Internet

Susan Schiavetta
University of Oslo
Norwegian Research Center for Computers and Law

Konstantinos Komaitis
University of Strathclyde

1. Introduction

Social control is a normative process whereby societies introduce rules that shape their existence and internal and external relations.[1] In many ways, controlling information within a society is an essential part of the process of social control, as it serves to prevent the proliferation of thoughts and expressions that can undermine a society's overall goals. Controlling information therefore, is not something new; rather it has always been used as a strategy to determine the direction in which societies should move. In the online environment the phenomenon of controlling information takes on new dimensions. Since the Internet is a zone that knows no national boundaries, no government can reign autonomously over it, yet governments have managed to come together to exert some control. A prime example of this control lies in the management of the domain name system (DNS) by the Internet Corporation for Assigned Names and Numbers (ICANN). In particular, the mandatory character of the Uniform Dispute Resolution Procedure (UDRP), the decisions taken in cases heard under the UDRP regarding freedom of speech, and the operation of the WHOIS database all serve to exemplify the control ICANN has over information on the Internet. Accordingly, each of these issues will be analysed in turn so as to ascertain the exact power that ICANN possesses, and the amount of influence that it has over information online.

2. ICANN's Raison D'être

In the years preceding ICANN's creation (1972 – 1998), Jon Postel, one of the Internet's founding architects, and the Internet Assigned Numbers Authority (IANA) documented the procedures for the DNS in a series of 'Request For Comments' (RFC),[2] which were adopted by the Internet Engineering Task Force (IETF). Although RFCs are non-binding they are widely recognised as the main source of Internet standards and hence they have a great deal of influence.[3] In 1994 Postel and his lawyer proposed that IANA be *"[t]he central coordinator for the assignment of unique parameter values for Internet protocols"*.[4] After reaching an agreement with the United States (US) Government, IANA became a clearinghouse for the DNS. Subsequently a number of RFCs were issued that documented IANA's new functions. Above all, RFC 1174 (later replaced by RFC 1591) portrayed IANA as the ultimate authority for the allocation of IP Addresses, the organisation of the DNS, and numerous other parameters used to support the Internet.[5]

Originally, on behalf of the US Government, the National Science Foundation (NSF) created InterNic; the INTEgRated Network Information Centre to provide services related to domain name registration. InterNic was made up of three existing organisations, Network Solutions Incorporated (NSI) which registered all non-military gTLDs, AT&T which handled the database services, and General Atomics which managed the information services side.[6] Although the latter two organisations had important functions, NSI was given the most significant role. *"[A]s of September 30, 1998, NSI had registered a total of 2,777,000 domain names and reaped gross profits of $35.9 million"*.[7] With an increase in Internet traffic and greater international exploitation, tensions grew in respect of this American monopoly, particularly in light of such profit margins. Consequently, foreign governments called for the US Government to reflect the global characteristics of the Internet by decentralising the DNS management functions so that no government would single-handedly control the Internet.

2.1 ICANN

In 1997 the US Secretary of Commerce was instructed by the Clinton Administration to privatise the management and operation of the DNS.[8] After the release of a Green Paper which stimulated intensive discussions,[9] a White Paper was published by the Department of Commerce (DoC) calling for the incorporation of a *"[n]ot-for-profit corporation managed by a globally and functionally representative Board of Directors"*.[10] Following the release of a Memorandum of Understanding (MoU) on the 25th of November 1998, ICANN - the organisation proposed by Postel to take executive responsibility for the technical aspects of the Internet - was recognised as such.[11] Four principles explicit in the MoU were stability, competition, private bottom-up co-ordination and representation. The stability principle recommended that both parties work together to ensure that the management functions that had previously been operated by, or on behalf of, the US Government would be transferred to the private sector without disrupting the stability of the Internet. The competition principle was geared at lowering costs, promoting innovation, and enhancing user choice and satisfaction. Bottom-up co-ordination focused on private sector action as opposed to government control. The representation principle required that the functional and geographic diversity of the Internet and its users be reflected through the technical management of the DNS.[12]

At the outset ICANN's Board of Directors were self appointed and supposed to work on an interim basis for a fixed period of one year. In addition they had the task of electing and installing a replacement Board.[13] Early bylaws produced by the interim board stated that they would continue to serve as nine At-large members until they were replaced. The nine new At-large members were to be elected by Internet users that had At-large membership status so as to ensure that the decision making process embraced international stakeholder participation. To obtain an At-large membership the applicant had to be over sixteen and have both an email account and a postal address.

The transition from the interim Board to the new one also involved the number of members sitting on the Board being extended to nineteen. Nine of the new members were to be appointed by ICANN's Supporting Organisations, with the final post being filled by a President.[14] Even after the Supporting Organisations had elected their directors, the interim members became a more permanent fixture. In accordance with the original by-laws they extended their term of office to 30th September 2000, but tensions grew in respect of this so-called 'Board Squatting'.[15] Public online elections were eventually held for five of the nine At-large posts and hence there is now at least one representative from Africa, Asia/Australia/the Pacific, Europe, Latin America/the Caribbean, and North America.[16] The other four At-large seats have never been put up for election and as a result four of the original interim board members remained on the Board, although one stepped down in December of 2002.[17]

Currently ICANN is reforming itself, with both the composition of the Board and the electoral process being revamped.[18] In respect of composition, the new Board is to consist of fifteen voting members and six non-voting liaisons. One of the main changes to the electoral process relates to the rejection of public online elections for the At-large posts as a result of problems associated with

fairness, representation, validity and cost.[19] As such the election process will involve eight of the voting members being selected by a Nominating Committee that is composed of voting and non-voting members from the various Supporting Organisations and Advisory Committees. In particular five of the voting delegates on the Nominating Committee are selected by the At-Large Advisory Committee (ALAC) - the new At-large structure.[20] Thus, no At-Large members will actually sit on the Board of Directors; rather their role is limited to mere participation in the electoral process itself which is regrettably a diluted version of stakeholder participation.

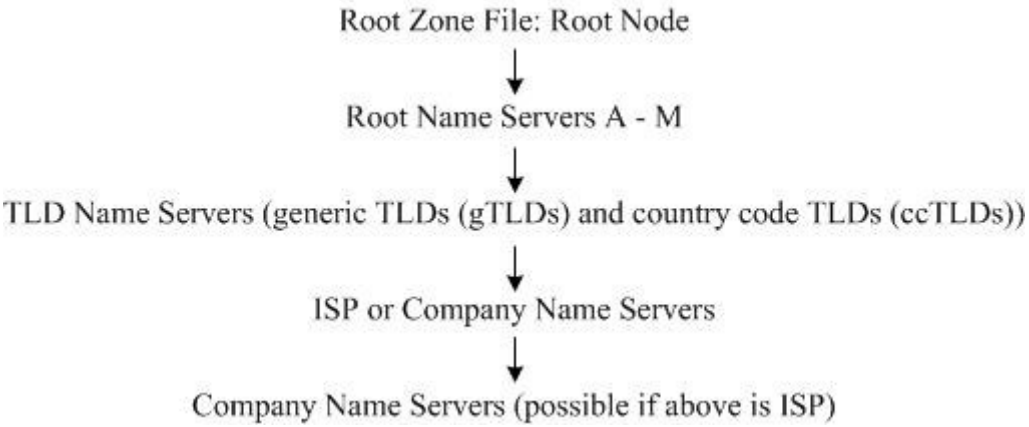
Six of the remaining Board members are selected by the Address Supporting Organization, the Country-Code Names Supporting Organization and the Generic Names Supporting Organization. The final voting Board member is the President, and s/he is chosen by the Board itself.[21] In respect of the non-voting liaisons these are appointed by the various Advisory Committees and the IETF, with one being selected by the Governmental Advisory Committee (GAC). During the voting process, the electors must aim to pick individuals with integrity, objectivity and intelligence, an understanding of ICANN's mission and its potential impact on the Internet, and a good knowledge of the DNS. Moreover, the members must reflect the broadest cultural and geographic diversity possible so long as the other criteria set forth are met.[22]

2.2 ICANN's Real Power

Whilst the overarching aspiration of the privatisation process was to have a self regulatory type body that would have complete autonomy from the US Government this has not really been achieved. ICANN still remains partially under the control of the DoC, and is therefore subject to government intervention. Most of the DNS infrastructure is owned by the US Government as a consequence of their original funding efforts, and accordingly they have the right to set the conditions under which the privatisation process proceeds. Correspondingly the MoU states that prior to completing the transition to the private sector, the DoC, on behalf of the US Government, must have assurances that the private sector has the capability and resources to assume the important responsibilities related to the technical management of the DNS.[23] Hence, the DoC and ICANN must collaborate in respect of certain functions. In particular, the DoC has a duty to oversee the operation of the authoritative root server system and policies.[24] Over and above this, the DoC has a more general duty to monitor the various activities of ICANN.[25]

Claiming ultimate policy authority over the root zone is the most important aspect of the DoC's role. Since the DNS is a hierarchical, distributed, interdependent system that requires unique addresses, it makes it impossible for two identical domain names to exist simultaneously. Residing at the top of this hierarchy is the root zone file, which contains a list of thirteen computers (root name servers). These root servers are currently identified by letters A-M, with the primary root zone file being located on the A root server.[26] Taken as a whole, this system is known as the root zone. Root servers hold the master lists (Root Files/DNS Records) of the Internet Protocol (IP) numbers for the Top Level Domain (TLD) name servers. Likewise, each TLD name server holds a database of DNS Records of registered name servers and their associated IP numbers. Domain names are resolved by sending a query to the name server selected by the user or their Internet Service Provider (ISP). If the data is not in the name server, the query works its way up the chain until it can be resolved.[27] Diagram 1 below gives an overview of the DNS hierarchy.

Diagram 1



Overall control of the root server equates to substantial economic and political power, as whoever controls the DNS decides what new suffixes will be added to the root server and the way in which names and essential routing numbers will be assigned to websites and other Internet sources. Generally speaking ICANN has no authority when it comes to making final decisions on the address system of the Internet, as the DoC must first give their approval. This is true for both gTLD and ccTLD re/delegations. Prior to 2000 IANA was responsible for providing the technical coordination services to all Internet users, but after ICANN submitted a proposal to the US Government, the administration function associated with root management, including receiving, investigating and reporting on re/delegation requests - the so-called IANA function - was transferred to ICANN.[28] At no time however was ICANN authorised to modify, add or delete information held in the root zone, rather this function remained with NSI (now a subsidiary of Verisign).[29] Thus, any changes to the root zone file must be supported by the written direction of an authorised US Government official and carried out by NSI.[30] As long as the DoC retains this last word authority, they continue to have a great deal of power when it comes to the operation of Internet.[31]

Yet ICANN acts as if it has full control over the DNS, particularly since it carries out the day to day functions assocciated with the DNS. ICANN's tasks also include coordinating the assignment of Internet technical parameters which maintain universal connectivity on the Internet, performing and overseeing the functions related to both the co-ordination of the IP address space and the Internet DNS, supervising the operation of the authoritative Internet DNS root server system, and engaging in any other related lawful activity in furtherance of these functions.[32] ICANN's role is so great that even though the US Government has the power to withdraw its authorisation at any time, it does not want to take responsibility for the routine running of the DNS. As such, the DoC retains more of a supervisory function than anything else; merely rubber-stamping anything that ICANN does that relates to the technical management of the DNS.

ICANN's role as regards setting the criteria to be followed when admititing new TLD suffixes to the root is particularly exemplery of its real power. As witnessed during the recent gTLD additions, ICANN selects which applicants have made a viable proposal for a new gTLD and then the DoC gives its consent. Upon gaining the stamp of approval ICANN enters into contractual discussions with the new TLD operators. In respect of ccTLDs the approval process is more predictable since ICANN is not in the business of deciding what is and what is not a country and the US Government has already acknowledged a role for national governments in respect of managing and establishing policies for their own ccTLDs. Thus, as long as the International Standard 3166 is met ccTLDs will gain backing from ICANN to enter the root. Nonetheless, ICANN must still support a ccTLD entry. Accordingly, from this perspective, it is more important who decides what goes into the root zone file as opposed to who gives the final authorisation or operates the computer that is the source of that file.

In a similar vein, ICANN's exclusionary conduct towards competitors, i.e. companies who wish to have an active role in the gTLDs registrations, in particular its treatment of New.net Incorporated reflects the power that ICANN has. ICANN made it clear from the beginning that New.net

registrations would never make it into the root zone file. Andrew McLaughlin, ICANN's Senior Advisor, questioned New.net's legitimacy and accused it of harbouring a vision that could bring chaos to the Internet. It is suggested that ICANN's opposition to New.net derives from the fact that New.net has managed to capture some rather appealing domain names, not to mention customers. Essentially New.net domain names are directed to an alternate root, which is secured through agreements with various ISPs. Ultimately however, unless New.net accepts both the authoritative root and ICANN, their domains names will never make it into the root zone and hence they will never be universally resolvable.[33]

2.3 ICANN's Future as DNS Manager

Many people have been dissatisfied with the way in which ICANN has hitherto carried out its functions, suggesting that it has been too secretive, not accountable enough to Internet users, businesses and other key interest groups, and has exceeded its authority on numerous occasions. Such a view of ICANN is epitomised by the recent bill proposal by the US Senator Conrad Burns, who suggested that the US government should have more influence over ICANN than it already has so as to ensure appropriate scrutiny. Unfortunately such an approach would only make things worse, with ICANN already coming under fire for being too US-dominated. If the US government were to exert more control *"[i]t could be seen as an effective annexation of the internet [sic]"*.[34]

Whilst the US Government may never give ICANN complete freedom to run the DNS,[35] other governments do have ways of influencing ICANN's activites. For instance, international bodies, such as World Intellectual Property Organisation (WIPO), can be used as a tool to introduce governmental agendas into ICANN. Likewise the GAC also helps governments get involved. Indeed, the current reform process reflects the fact that governments are going to be even more involved via the GAC. At the moment the GAC only has the ability to consider and provide advice on the activities of ICANN by reporting promptly to the Board through the Chair of the GAC,[36] but this is due to change with GAC representatives being able to participate in discussions, debates and meetings, although they will not have the right to vote. Above all, when the reform process is completed rather than just reporting to the ICANN Board the GAC will have one member that actually sits on the board.[37] Such a role for the GAC was deemed necessary because it was *"[s]imply unrealistic to believe that global coordination of the [DNS could] succeed without more active involvement of governments"*.[38] Of course the optimal position is freedom from one distinct government with all governments, including the US, having equal participatory powers.

In fact the real path to success is a public/private partnership that allows the private sector and global governments to co-operate under the umbrella of an organisation like ICANN so that all opinions are taken into consideration and decisions are taken in a timely fashion. Whilst many fear government involvement, in reality such an approach is essential because the Internet is increasingly critical to the social and commercial well-being of the citizens of all countries.[39] Consequently, in contrast to other harmonisation efforts, such as the Convention on Cybercrime, governments from around the world have basically sanctioned the realisation of an international body to manage the Internet - a Cyber Government if you will - that aims to realise the goal of public/private collaboration. When this has been achieved governments and Internet users alike will be able to exert equal influence over the activities of ICANN.

However, this may only be a utopian view of what can be achieved through ICANN, and as things stand now, ICANN acts more like a chameleon changing its colours to suite its environment, protecting itself from its enemies. Sometimes ICANN presents itself as a private entity that shields the Internet community from national control and on other occasions it chooses to act more like a governmental body that co-operates with the GAC.[40] This metamorphosis is neither desirable nor sustainable. Accordingly, unless ICANN's role is defined by a self regulatory system that produces equal accountability to all, ICANN may be forced to move under the auspices of one of the existing standards organisation with international representation, such as the International Telecommunications Union or be turned into a treaty organisation with a body like the GAC acting

as its principal. Pending a decision as to ICANN's future role, the DoC will continue to act in its capacity as a 'dormant authority' that serves to legitimate ICANN's activities until the correct model is found that allows sufficient accountability and a stable transfer to the private arena.

Despite this uncertainty looming in the background, the underlying theories which led to ICANN's launch were sound nonetheless. Accordingly ICANN will more than likely continue as the organisation that manages the DNS for the foreseeable future. If it is to maintain this position some fine-tuning is required. Governments obviously have a responsibility as regards steering ICANN but it must be borne in mind that they represent both their citizens and businesses and other entities within their borders. Hence, members of the general public must also have some method by which they can make themselves heard. ALAC is meant to fulfil this role, but as noted it has a limited role in respect of the Board of Directors and, furthermore, membership is not open to the public, but rather organisations. The ten member strong panel that comprise ALAC are supported by a network of self-organising 'At-large Structures', which are organised into 'Regional At-large Organisations'. At best the Regional Organisations must manage outreach and public involvement programs with a view to getting some public input. Consequently this is an element of ICANN's representative function that must be explored further. One suggestion is to open up the membership to members of the general public, so that individual users, academic institutions, non-commercial entities of various kinds, including consumer groups, and non-governmental organisations can all participate.

3. The Uniform Dispute Resolution Procedure (UDRP)

Notwithstanding the fact that ICANN's responsibilities are subject to external restraints, ICANN has still managed to put systems in place that allows it to exert a certain degree of control over online activities. One such system is the UDRP which was created to resolve disputes between trademark holders and domain name owners. Originally NSI operated a dispute resolution procedure for the resolution of such disputes because it had the responsibility for handling domain name registration services, but this procedure was deemed inequitable. Trademark owners had to prove that the trademark was registered prior to the domain name; hence non-registered trademark holders could not secure protection. When ICANN took over the technical coordination of the DNS it replaced this system with its own. WIPO was drafted in to prepare a report on how domain name disputes could be settled more efficiently and equitably. The desire for a swift resolution and the fact that WIPO's report was only advisory in nature meant that WIPO did not follow normal procedures when preparing the proposals. Rather it limited the direct involvement of Member States to the occasional status report and opening its public consultation sessions to government speakers. Thus, after meeting with intellectual property stakeholders and the like to acquire information and advice, WIPO drafted the proposals alone.[41]

Based on WIPO's recommendations,[42] ICANN adopted a mandatory dispute settlement system for *"[...] deliberate, bad faith, abusive domain name registrations or cybersquatting"* on the 24th of October 1999.[43] Coming into force on the 1st of December 1999, the UDRP boasts a very influential set of rules, covering disputes involving gTLDs. Currently four organisations have been approved for settling domain name disputes under the UDRP; these are the Asian Domain Name Dispute Resolution Centre, the CPR Institute for Dispute Resolution, the National Arbitration Forum (NAF) and the WIPO Arbitration and Mediation Centre.[44]

Paragraph 4a of the UDRP Policy states that a domain name holder (respondent) must abide by the rules in the event that someone (complainant) has suggested that:

- The domain name held is identical or confusingly similar to another to which the complainant has rights;
- The domain name holder has no rights or legitimate interest in the domain name; and
- The domain name has been registered in bad faith.

During the proceedings the burden of proof lies with the complainant to confirm the existence of these three elements, although it is the third element that is the most important and divisive. Four examples are given in paragraph 4b as to what can constitute bad faith; these are cybersquatting, maliciousness, anti-competitive practices, or free riding, although this list is non-exhaustive[45] Moreover, paragraph 15a gives panellists the discretion to apply any rules and principles of law they deem applicable to the dispute. Subsequently, panellists can effectively formalise radical decisions as to what constitutes bad faith and what legal system can be used and hence the possibility for inconsistency and wide interpretations is rife.

Once a complaint has been made concerning a possible conflict between a domain name and a trademark, no action can be taken until a neutral decision-maker has given a ruling. Such a decision-maker can be either a panellist registered with one of the approved dispute settlement providers, or a judge operating within a court of law.[46] A complainant can choose to proceed solely with the UDRP system to see how things evolve, or they can choose to invoke legal proceedings. Thus, whilst the UDRP is mandatory in the sense that the respondent must submit to the UDRP, this does not prevent litigation being launched either before UDRP proceedings have commenced, during the proceedings or within a ten day period after a decision has been given.[47] As a result this process represents compulsory participation for the respondent as opposed to compulsory binding dispute resolution for both parties. Indeed, the very fact that a UDRP panellist can find in favour of a complainant as a consequence of a no show by a respondent supports this analysis. Only when neither party decides to bring proceedings in a court within the ten day limitation period will the decision given by a UDRP Provider be binding on both parties.[48]

3.1 The Mandatory Character of the UDRP

When devising a dispute resolution system for domain name disputes, the main objective was to create a cheap, fast, and advanced solution to the problems associated with multi-jurisdictional disputes.[49] Making the UDRP mandatory seemed essential to ensure that the system would achieve these goals. Thus, when ICANN adopted the UDRP, it imposed the procedure on all registrars operating with .com, .net and .org TLDs. As a corollary of this, all registrars had to insert a third-party beneficiary clause into all their registration contracts in favour of any entity that believed that a registrant's domain name registration was in direct conflict with their trademark rights. Pursuant to this, NSI was not allowed to list any registrations in the root zone file where a registrar had failed to adhere to this policy. Consequently ICANN ensured that all registrars would comply and that the dispute resolution system would succeed.[50]

As for the decisions made under the UDRP by panellists operating for the approved dispute resolution providers, ICANN does not officially accept any responsibility for them.[51] Likewise, the four providers do not consider themselves accountable for the actions of their panellists. Taking into account that the UDRP is a mandatory system this is a rather questionable situation. Indeed, since ICANN created the final version of the UDRP it can be suggested that they should also be responsible for the effects of UDRP judgments, particularly when they are the only organisation that has the power to amend the UDRP in response to problems encountered.

Essentially ICANN has created a form of control via the UDRP, and the panellists are merely executing the system. Thus, whether or not ICANN actually decides which domain names should be transferred is irrelevant. To be sure, the root zone can be used to enforce the decisions taken on its behalf by the panellists and hence ICANN has the ultimate enforcement tool. Whilst registrars are obliged to implement the decisions of UDRP panellists by making the necessary amendments to their name server and database, ICANN also has the power to initiate a change to a domain name registration.[52] Furthermore, since the IP addresses of all TLD name servers need to be stored in the root zone servers and all IP addresses of name servers are stored on the TLD servers, technically the root zone plays a major part regardless.

As Lawrence Lessig has illustrated, the architecture of the system is very important, as it can

function in such a way that it serves to regulate people's behaviour.[53] This argument is particularly valid here in that the operation of the DNS via the root zone determines who can enter the Internet, and how long they will stay. In this sense, the power of controlling information is the thin line between its creation and destruction. Accordingly, the three powers of a government are operated by or on behalf of ICANN, with ICANN itself taking up the role of legislator, the panellists acting as the judiciary, and the registrars being the executive.

Further support for this argument comes from the relationship between ICANN and ccTLD registries, in that all ccTLD registries must also implement a mandatory dispute resolution procedure. ICANN has been prudent and refrained from interfering with the type of dispute resolution procedures that national registries should implement, although they have, through WIPO, produced a best practice guide based on the UDRP.[54] Since many small or unsophisticated registries want to avoid being burdened with having to create their own policies they look to ICANN's UDRP for advice. Whilst some, like Nominet, the UK registry for domain names ending in .uk, have chosen not to use the UDRP as a template, the fact remains that a significant number do, and thus ICANN indirectly controls the way in which disputes are handled in those countries. As such, many of the decisions taken by panellists operating under ccTLD dispute resolution systems will be in line with UDRP panellists. Given that all ccTLD registries maintain the appropriate name servers and zone files for their respective ccTLDs,[55] ccTLD managers determine which domain names will be visible in cyberspace in accordance with the decisions of their panellists. Thus, the implementation of these decisions very often reflects ICANN ideology.

3.2 Controlling 'freedom of speech'

Similarly, the phenomenon of dot-sucks cases also holds some particularly interesting connotations as regards the manifestation of controlling information. Dot-sucks domain names consist of all those domain names which criticise or satirise well-known trademarks. Even where registrations of dot-sucks domains have not been for commercial gain, panellists have ruled that they are considered to be confusingly similar in the eyes of consumers nevertheless and as such they have been registered in bad faith. Subsequently, dot-sucks domain names have habitually been transferred to trademark holders. The most worrying aspect of this form of information control is that it collides with the fundamental constitutional right of free speech, which would, in the offline world, only be overridden in the very rarest of situations. Indeed, in almost every region around the world, most - if not all - protests made via dot-sucks web sites would be protected under free speech laws, even if they were potentially confusing, so long as they were purely non-commercial.[56]

The **Dixons-online.com** case offers the greatest insight into the misapplication of the UDRP rules by panellists as regards freedom of speech.[57] In this case the respondent ran a consumer complaints service about Dixons for which no charge was made. The panel found that whilst there was no evidence to suggest that the respondent offered goods or services for commercial gain, the use of the domain name was nonetheless illegitimate.[58] In support of their decision they stated *"[t]hat 'competitor' has a wider meaning and is not confined to those who are selling or providing competing products. In this wider context it means, 'one who acts in opposition to another and the context does not demand any restricted meaning such as commercial or business competitor'. [Since] the respondent is competing with the Complainant for the attention of Internet users, [this] clearly has the potential to disrupt the Complainant's business"*.[59]

In view of the fact that the Internet has become a principal medium for exchanging information, and thus activating freedom of expression rights, it is suggested that this is a particularly overt way of controlling information.[60] To be sure, the majority of domain names that are of a derogatory nature will be true protests, and where they are not, the bad faith element will shine through. Moreover, the approach taken by many of the UDRP panellists is somewhat condescending as it reflects that they think consumers are not intelligent enough to distinguish between a site that a company has supported and a site that a disgruntled consumer/employee has launched. Certainly it is for these very reasons that some panellists have abstained from applying the UDRP rules in this way.

For instance in **Lockheed Martin Corporation v. Dan Parisi**,[61] a panel ruled that trademark attached to the term 'sucks', or any other critical phrase, makes it very obvious that the trademark owner has not authorised the site, and consequently no confusion will arise. This particular decision was based on a United States Federal Court ruling,[62] which explains the move towards supporting free speech in the domain name context.

Likewise, in a more recent case involving the UK supermarket chain Asda, a panellist strictly adhered to the UDRP rules and upheld free speech rights. In this case an employee of Asda registered the domain name asdasucks.net to create a site on which he would air his grievances about the company's managerial abilities.[63] When the supermarket brought the case before WIPO's Arbitration and Mediation Center, the site had never been exploited, but since the employee was already operating a similar web site, bearing the domain name asdasucks.co.uk, the panellist chose to analyse it for comparative purposes. On the operative site a notice was displayed that indicated that the site was in no way connected with the supermarket, but rather active for dissatisfied employees. On this basis it was assumed by the panellist that the complainant would use the asdasucks.net site for the same purposes. The panellist also reasoned that, on the balance of probabilities, it was doubtful that the asdasucks.net site would confuse Internet users into believing that the site was a product of Asda itself. Any disruption to Asda's business would therefore be minimal and accordingly the issue was not worthy of consideration. The panellist added that whilst he took no pleasure in dismissing the complaint because the material on the active site was *"[s]candalously and disgustingly abusive"*, a broader interpretation of the dispute resolution policy rules would be risky. [64]

The problems encountered in respect of the clash between free speech rights and the interpretation of bad faith registrations has been overcome entirely by Nominet. In 2001 Nominet restructured their dispute resolution system for domain name disputes. In particular, Nominet's procedure now includes a fair use clause which means that dot-sucks registrations that are considered as 'true protests' will be permitted. Thus, while the UDRP rules have given panellists too much latitude as regards defining bad faith, which has resulted in free speech rights being curbed on the Internet, progress is being made nonetheless. ICANN should learn from Nominet's approach while taking into consideration the reasoning of recent panellists. Indeed, with some panellists remaining flexible as to what constitutes a true protest the dot-sucks phenomenon will remain in a state of flux.

On the whole therefore, whilst some panellists have moved away from restricting freedom of speech rights the dot-sucks phenomenon reflects that the power exists to control information online all the same. ICANN may not take responsibility for the panellists that administer the system but as said they did create the system and are the only body able to change it and hence they are indirectly responsible for its effects.

4. The WHOIS Database

Another naked expression of ICANN's control over information online stems from the data being collected by registrars during the registration process. When a domain name is registered, the registrar must record the domain name along with the registrant's personal contact information, such as name, address, phone number, and e-mail address in their registrar database. This practice is system-wide for all registrars registering gTLDs. NSI then correlates the information held by the various registrars into a registry level database, known as the WHOIS. When NSI obtains information on new registrations, unique handles are assigned to them. The WHOIS service provides a means by which to search the domain name and handle fields.[65] For transparency reasons this database is in the public domain and current practice dictates that there is no way to prevent the information contained therein from being displayed.[66] When the WHOIS database is searched it will return information on the owner, the administrator, the technical contacts, and the name servers for a registered name. It may also indicate which registrar registered the domain name and the date on which it was registered and/or renewed. If a WHOIS search returns with an answer like 'record not found', this usually means that the name has not yet been registered, but since the information is

not updated in real time, such a reply is never one hundred per cent accurate.

Without a doubt the WHOIS database is a crucial tool for law enforcement bodies, panellists applying the UDRP rules, owners of Intellectual Property (IP), domain holders themselves and by the average Internet user who may wish to either check the availability of a domain name or validate a holder for consumer purposes. However, this mechanism can be easily misused by those who wish to send unsolicited commercial e-mails or commit crimes such as stalking. Primarily problems stem from the fact that domain name registrants are making their personal data available to anyone searching the WHOIS database, which effectively leads to registrants renouncing any data protection rights they may have and making their personal data available for all to see. This quandary is particularly pertinent for individual registrants, and above all EU/EEA citizens covered by the strict Data Protection Directive.[67] Thus, whilst the WHOIS database is a good tool for checking the particulars of a domain name holder, the point is should such information be accessible and if so, to whom should it be accessible? Such a query becomes even more relevant when it is considered that very often domain name registrants do not realise that the information they supply is made available to the public in a searchable database.

A particular example of this loss of privacy rights for EU/EEA citizens relates to the transfer of registrant's personal information to NSI in order to update the WHOIS. NSI operates within the boundaries of the less demanding US data protection legislative framework, and as such EU data subjects are supposed to give there consent to such a transfer, but regrettably registrants are not given the opportunity to consent. As the UK government has indicated where there is no real choice in the matter consent is unlikely to be valid.[68] Furthermore, consent must be freely given in that the individual must be able to decline without suffering any consequences, which is clearly not the case here since to get a domain name a registrant must agree to give up their personal information. However, it may be possible for the WHOIS database to fall under one of the exemptions, for instance, Article 26 (3), which allows derogations where the processing is necessary for the performance of a contract or in order to enter into a contract requested by the data subject.[69] Nonetheless, the right to privacy is still valid even for those who start out with minimal privacy protection.

Ultimately, where an individual operates a website for purely personal purposes then they deserve to be shielded from the possibility that their data will be misused. Realistically though, only a few websites will meet the ideal of a personal endeavour. Additionally, it can be difficult for a registrar to pre-determine which sites are personal and which are not. Certainly, a lot depends on the information supplied by the registrant; and where a registrant is found to be dishonest their rights to the domain name will be lost. The fact remains however that some information should not be open to the public. Unfortunately though, by revealing personal information through the WHOIS individuals are availing themselves to direct marketers and such like. What is more, depending on the content of the website, information on the registrant's sexual life, religious beliefs or trade union membership may be revealed indirectly. As a result the WHOIS database significantly hampers the individual's ability to be 'a dog' in cyberspace.

As regards web sites that are e-commerce based, it is much easier to determine how much information should be available as why should a company have a right to keep their place of business a secret? A company must be easily accessible by everybody in order to become known and establish trust. Thus, websites conducting e-commerce should have little influence in respect of how their information is controlled.[70] Such an approach is epitomised in the Distance Selling and the E-commerce Directives that apply throughout the EU/EEA, whereby businesses are required to publish their contact details under certain circumstances and in certain manners.[71]

Article 4 of the Distance Selling Directive, for example, states that prior to the conclusion of any distance selling contract that the supplier must furnish the consumer with their identity and were payment is requested in advance their address. Similarly Article 5 the E-commerce Directive states that service providers must ensure that their name and geographic and email addresses are easily and

permanently accessible. Accordingly the fact that the WHOIS database contains contact information on businesses is irrelevant since they have to display it anyway if they intend to trade. Although there is an argument that Article 4 of the Distance Selling Directive becomes superfluous since the contact information of a business is available to consumers through the in the WHOIS database whether or not they enter into a contract with them. However, when it is considered that the contact details published by businesses in the WHOIS often belong to technical and support services, this argument becomes largely redundant.

4.1 Reforming the WHOIS

In an effort to address privacy concerns ICANN established a WHOIS Task Force to analyse the efficiency of the system. Recently a Final Report was issued entitled 'Accuracy and Bulk Access' which allowed a 10-day period for comment.[72] Implying that accuracy of WHOIS data supersedes legitimate privacy interests, the Report failed to recommend appropriate privacy safeguards for domain name registrants. Rather the Task Force decided to leave privacy concerns to a separate report. Whilst this was disappointing it has been suggested that it may be a strategy to achieve consensus on privacy-free aspects, as opposed to delaying agreement on everything as a result of an absence of consensus on privacy issues.[73] Moreover, whereas privacy concerns are undoubtedly very important, the accuracy of the data in the WHOIS is also a major issue since data must be accurate for the system to be functional. Nevertheless, such an approach may lead to many legitimate privacy issues being dealt with unsatisfactorily.

Even though the WHOIS is actively being discussed, the extent of change to the WHOIS is far from clear at this point. Whereas, IP right holders are pushing for greater accuracy and the preservation of the system as it is, non-trading individuals and various other commentators are demanding that personal information be protected against misuse. Undoubtedly when attempting to meet the requirement of transparency, the question of non-discrimination cannot be avoided. This does not however mean that there are not ways to ensure that both requirements are satisfied, as the results obtained after submitting a WHOIS query can easily be controlled. Instead of showing all the information pertaining to domain name registrants, the results could simply reveal whether a domain name exists, whether it is active and the name of the registrant. After that, if someone would like to have more details this could be done via the registrar, with the enquirer having to give some minimum identifiers in order to obtain the requested information. Nevertheless, this option would require different (possibly more advanced, yet available and easily implemented) software and network applications and the creation of a WHOIS Enquiry Services, which would more than likely be quite costly.

Whilst it is likely that ICANN will develop a more balanced approach that adequately protects the privacy of those listed in the WHOIS that still allows good access for bona fide WHOIS users, it may be sometime before this is achieved. Advantageously things may move quicker now that the new President of ICANN (and founder of PrivacySolutions) Paul Twomey is very interested in privacy rights.

4.2 Nominet and the WHOIS

Is a similar way to gTLD registries, every ccTLD registry must keep records of those registering domain names with them, although ccTLD regstries are not subject to any uniform rules as regards what information must be compiled. Various ccTLD registries have found solutions to the problems that face ICANN, for instance some do not make their databases available for search, but merely tell you whether or not the domain name is available and others simply refuse to allow private persons to register domain names. The most interesting approach is that of Nominet who recently amended the rules in respect of what information is recorded in its WHOIS database. Originally it planned to expand the information accessed and returned to: the registrant's name, address, the name of the registration agent, the address of the registration agent, the date of registration, the last time the registration was updated, the date it is due to be renewed and the name server information, but this

was not met by support from the Internet community. Consequently the proposal was modified so that it would only be compulsory for those classed as businesses to show their address. Non-trading individuals would thus be able to opt-out of publishing such information via their ISP or registration agent.

The changes took place in two phases, with the first phase beginning on the October 1st 2002 and the second on December 1st 2002. The first phase involved all the required fields going live, apart from the address details of non-trading individuals. The second phase consisted of the address details of all those domain name holders either registering or renewing a domain name being included in the WHOIS. As a part of this phase all non-trading individuals had the ability to opt out. Ordering the changes in this way allowed the address details for existing non-trading domain name holders to be left out until the month in which their domain name was due to be renewed. Where a non-trading domain name holder has opted out the address field will read: *"[T]his individual has chosen to opt-out of the WHOIS. Contact via Agent".[74]* In order to be classed as a non-trading individual the domain name must not be used for any business activity. In line with UK legislation that implements the Distance Selling and E-commerce Directives, there will be no opt-out for domain names that are classified as businesses.[75]

4.3 Nominet v. ICANN

It is suggested therefore that if Nominet can manage to implement two different systems for trading and non-trading domain name holders then so can ICANN. Indeed Nominet's system seems to be the most balanced approach, as it allows individuals to retain their privacy whilst guaranteeing that IP right holders, consumers, etc have the means to make contact with and explore the information held on domain name holders. As Karl Auerbach has observed, ICANN's current position in respect of the WHOIS database is nothing more than a repudiation of the idea of personal privacy. Whilst individuals who believe that their rights have transgressed, including IP right holders, should have the ability to prove that their rights have indeed been violated, the access rights of those alleging infringement should also be limited to looking at information pertaining to those accused. Furthermore guarantees should be established that ensure that the information being analysed is not used for purposes other than the inquiry. An aspect of this may require those making the allegations to leave trustworthy records of their identity and of the nature of the data they examined so that those being examined also have the ability to right a wrong.[76]

5. Conclusion

The question of who controls the Internet is directly related to the question who wants to control the Internet. From the moment that the Internet was opened up to commercial activity many different groups wanted to dominate, such as users, communication companies, ISPs, and governments. Of them all the most objected to was government intervention, yet it is governments that have managed to exert the most control. In particular the US Government has a substantial power over the Internet given that it has the ultimate authority over the DNS and above all the root zone. To overcome this US control ICANN was established to act as the Internet's manager, but as of yet the US Government still has the last word authority and hence the power to influence ICANN's actions; although other governments are increasingly making head way to infiltrate this.

Hopefully ICANN will eventually become autonomous from the US Government and all governments will be placed on a level playing field which allows them to contribute to the management of the DNS equally. Likewise the numerous other stakeholders should also have a greater role in the decision making processes of ICANN. Ultimately, ICANN can be a very successful medium for organising the Internet for the benefit of all but only if there is equal public and private participation. If this occurs ICANN's role as the Internet's Government will be more defined, and as such it will be able to operate more efficiently.

Despite a lack of autonomy in the interim, ICANN has a significant amount of responsibility and

has, as a result, managed to initiate a great deal of control over the 'inhabitants' of cyberspace. Hitherto, this control has proliferated through the UDRP and its operation, as well as the organisation of the WHOIS database. Whereas ICANN may not directly implement the controls itself, they are operated on behalf of ICANN nonetheless and accordingly ICANN wields a lot of power subtly, some might even say shrewdly.

---

[1] See further Social Control, Wikipedia Encyclopedia, http://www.wikipedia.org/wiki/Social_control (Accessed 11/02/02).
[2] See generally RFCs at Finding and Retrieving RFCs from the RFC Editor Site, Internet Society, at http://www.rfc-editor.org/rfc.html, (Accessed 21/01/02). In RFC 799 the creator of the DNS, Dr. David Mills, outlined the concepts and facilities required for an Internet Name Domains system that would eventually scale to facilitate addressing of "thousands of hosts".
[3] See generally Froomkin, Michael., Haberamas@discourse.net: *Towards a Critical Theory of Cyberspace*, http://www.law.miami.edu/~froomkin/discourse/ils.pdf, (Accessed 15/12/01).
[4] RFC 1700, http://www.armware.dk/RFC/rfc/rfc1700.html, (Accessed 04/02/02).
[5] RFC 1591, Domain Name Structure and Delegation, IETF, at http://www.ietf.org/rfc/rfc1591.txt, (Accessed 15/02/02).
[6] See further http://www.bangla.net/isp/tech_support/internet-timeline.html, (Accessed 25/01/02).
[7] *The Domain Name system: A Case study of the Significance of Norms to the Internet Governance*, Harvard Law Review, http://www.harvardlawreview.org/issues/112/7_1657.htm, (Accessed 10/03/02) http://www.harvardlawreview.org/issues/112/7_1657.htm.
[8] See further *A Framework for Global Electronic Commerce*, The White House 1997, http://www.nyls.edu/cmc/papers/whgiifra.htm (Accessed 10/03/02). See also Presidential Memorandum on Electronic Commerce, 33 Weekly Comp. Presidential Documents 1006 (July 1, 1997), which directs the Secretary of Commerce to transition DNS management to the private sector.
[9] See further *The* Department of Commerce Green Paper on a Proposal to improve the Management of Internet Names and Addresses, http://www.ntia.doc.gov/ntiahome/domainname/dnsdrft.htm (Accessed 10/03/02).
[10] See further *The* Department of Commerce White Paper on the Management of Internet Names and Addresses, (63 Fed. Reg. 31741(1998), http://www.ntia.doc.gov/ntiahome/domainname/6_5_98dns.htm (Accessed 10/03/02).
[11] See further http://www.ntia.doc.gov/ntiahome/domainname/icann-memorandum.htm, (Accessed 05/02/02).
[12] Ibid.
[13] See further *Supra* No.10. See also Mills, Elinor., *New Internet Body Elected*, http://www.nwfusion.com/news/1027icann.html, (accessed 31/03.03) and Wired News, *Meet the ICANN Board*, http://www.wired.com/news/politics/0,1283,15499,00.html, (accessed 01/02/03).
[14] See further Bylaws as at November 23 1998, http://www.icann.org/general/archive-bylaws/bylaws-23nov98.htm, (Accessed 28/01/02).
[15] See in particular Froomkin, Michael., *Beware of the ICANN Board Squatters*, http://personal.law.miami.edu/~froomkin/boardsquat.htm, (Accessed 10/03/02). See also Resolution 99.86 http://www.icann.org/santiago/santiago-resolutions.htm, (Accessed 12/02/02).
[16] See further *At Large Memberships and Elections*, http://www.icann.org/committees/at-large/at-large.htm, (Accessed 10/03/02).
[17] Geist, Michael., *Public's role in Net governance threatened*, June 13 2002, globeandmail.com, http://www.interesting-people.org/archives/interesting-people/200206/msg00067.html, (Accessed

24/02/02). See further *About ICANN*, http://www.icann.org/general/abouticann.htm, and Froomkin, Michael., *Supra* No.15. It was Frank Fitzimmons who stepped down. The remaining board squatters are:Hans Kraaijenbrink, Jun Murai, and Linda Wilson.
[18] Williams, Martyn., *ICANN President Calls for Major Overhaul*, http://www.computerworld.com/softwaretopics/os/story/0,10801,68604,00.html, (Accessed 10/03/02). See also Lynn, M, Stuart., *ICANN: The case for Reform*, http://www.icann.org/general/lynn-reform-proposal-24feb02.htm, (Accessed 10/03/02). See also Preliminary Report, ICANN Meeting in Accra, http://www.icann.org/minutes/prelim-report-14mar02.htm, (Accessed 12/02/02).
[19] Ibid.
[20] See further ALAC Announcement, http://www.icann.org/announcements/announcement-19feb03.htm, and Bylaws adopted 15th December, http://www.icann.org/general/archive-bylaws/bylaws-15dec02.htm, (Accessed 10/03/02), Article VI, Section 2 (1) and Article VII, Section (2).
[21] Bylaws, Ibid, Article VI, Section 2 (1). The current President of the Board is Australian Paul Twomey. He was picked by the current Board of Directors which is made up of Directors chosen under ICANN's old structure.
[22] Bylaws, *Supra* No. 20, Article VI, Section 2 (3).
[23] See MoU, Section II B, *Supra* No. 11.
[24] See MoU as amended (http://www.ntia.doc.gov/ntiahome/domainname/icann.htm), and in particular Amendment 5, http://www.ntia.doc.gov/ntiahome/domainname/agreements/amend5_09192002.htm, (Accessed 10/03/02).
[25] See MoU, Section V B (8), *Supra* No. 11, as reaffirmed by Amendment 5 Section I B (9), Ibid.
[26] See Peckham, Chris., *Comp.protocols.tcp-ip.domains*, Frequently Asked Questions, at http://www.intac.com/~cdp/cptd-faq, (Accessed 21/01/02).
[27]A name server is a network service that enables clients to name resources or objects and share this information with other objects in the network. Only when the name server starts from scratch will it contact one of the root name servers. If no caching has been done by the root name server then it will direct the name server to the .COM name server, and so forth.
[28] See further http://www.icann.org/general/iana-contract-09feb00.htm, (Accessed 10/03/02).
[29] See Special Award Conditions NCR-9218742 Amendment No. 11, http://www.ntia.doc.gov/ntiahome/domainname/proposals/docnsi100698.htm, (Accessed 10/03/02).
[30] See further Miscellaneous Section, Ibid.
[31] See for example, ccTLD Redelgation Step-by-Step Overview, http://www.iana.org/cctld/redelegation-overview-19jun02.htm, (Accessed 15/02/02).
[32] See MoU, Section II B, *Supra* No. 11.
[33] See further http://www.softwareuncovered.com/main.asp?url=/news/nbd-20010712.html (Accessed at 17/03/03). See also Wheeler, Janet., *New.net Distends Domain Dynasty*, http://www.isp-planet.com/hosting/2001/new_net.html, (Accessed 15/02/03).
[34] Millard, Elizabeth., *US to Seek Greater Control over the ICANN*, http://www.newsfactor.com/perl/story/18183.html, (Accessed 09/01/02).
[35] Koman, Richard., *Karl Auerbach: ICANN Out of Control*, http://www.oreillynet.com/pub/a/policy/2002/12/05/karl.html, (Accessed 10/03/02).
[36] GAC Operating Principles, http://www.noie.gov.au/projects/international/gac/docs/Operating_Principles-English.htm. See also http://www.icann.org/committees/gac/, (Accessed 21/02/02).
[37] Bylaws, *Supra* No. 14, Article VI, Section 9.
[38] Quoted in Williams, Martyn., *Supra* No.18.
[39] See Sims, Joe., "*ICANN attorney replies to Politech post on "self-regulation's end"*, http://www.interesting-people.org/archives/interesting-people/200206/msg00066.html (Accessed 12/01/03).
[40] Email communication with Mr. Karl Auerbach, March 13, 2003.
[41] Froomkin Michael.,, *ICANN's Uniform Dispute Resolution Policy – Causes and (partial) Cures*, Brooklyn Law Review, Vol. 67, No. 3, 2002.

[42] See further Statement of Policy on Management of Internet Names and Addresses. http://www.ntia.doc.gov/ntiahome/domainSee also ICANN Board Resolution 99.83, http://www.icann.org/minutes/minutes-26august99.htm, (Accessed 10/03/02) http://www.icann.org/minutes/minutes-26august99.htm. WIPO submitted its final recommendations (built on Interim Report) on 30th of April 1999. See further WIPO's Final Report; http://wipo2.wipo.int/process1/index.html, (Accessed 10/03/02) http://wipo2.wipo.int/process1/index.html.
[43] WIPO Final Report of the WIPO Internet Domain Name Process, Paragraph 135 (i), ibid.
[44] See further Approved Providers for Uniform Dispute-Resolution Policy, http://www.icann.org/dndr/udrp/approved-providers.htm, (Accessed 11/03/02) http://www.icann.org/udrp/approved-providers.htm.
[45] For more information on this issue see further Mueller, Dr. Milton., *Rough Justice: An Analysis of ICANN's Uniform Dispute Resolution Policy*, Convergence Centre,http://dcc.syr.edu/roughjustice.htm http://dcc.syr.edu/roughjustice.htm, (Accessed 24/11/01).
[46] Weade, Charlotte., *Trade Marks and Domain Names*, Law and the Internet: A framework for Global Electronic Commerce, Chapter 7.
[47] See further Uniform Domain Name Dispute Resolution Policy, http://www.icann.org/dndr/udrp/policy.htm, Paragraph 4 K. (Accessed 10/03/02) http://www.icann.org/dndr/udrp/policy.htm. If a decision by a court is requested before a decision has been delivered then the UDRP panel hearing the dispute may either stay the proceedings until a judgment is given, or continue with the case and give a ruling themselves. See Paragraph 18.
[48] See further Dluhos v. Strasberg No. 01-3713, see http://caselaw.findlaw.com/data2/circs/3rd/013713p.pdf (Accessed 21/02/03) and Ibid.
[49] See further Thornberg, Elizabeth, G., *Fast, Cheap and Out of Control: Lessons from the ICANN Dispute Resolution Process.*
[50] Froomkin, Micheal., *Wrong Turn in Cyberspace: Using ICANN to route around the APA and the Constitution*, 50 Duke L. J. 17, 2000.
[51] See further Paragraph 4 (h), *Supra* No.47.
[52] Paragraph 3 of the UDRP Policy, Ibid, states that ICANN can transfer, cancel, or otherwise make changes to domain name registrations upon receipt of written or appropriate electronic instructions from the registrant or authorized agent to take such action, upon receipt of our receipt of an order from a court or arbitral tribunal, or upon receipt of a decision of an Administrative Panel requiring such action in any administrative proceeding to which the registrant was party and which was conducted under this Policy or a later version of this Policy adopted by ICANN, or if necessary to conform with the terms of a Registration Agreement or any other legal requirements.
[53] See Lessig, Lawrence., *Code and other laws of Cyberspace*, Basic Books, 1999, First Edition.
[54] See further http://ecommerce.wipo.int/domains/cctlds/bestpractices/index.html, (Accessed 10/03/02).
[55] Best Practice Guidelines for ccTLD Managers, http://www.centr.org/docs/legal/best-practice.html, (Accessed 10/03/02).
[56] Froomkin, Micheal., *The collision of trademarks, domain names, and due process in cyberspace, Communications of the ACM*, February 2001, Vol.44, No.2.
[57]Case D 2001-0843.
[58] See further WIPO Final Report, *Supra* No.43.
[59] See further Thornberg, Elizabeth, G, *Supra* No. 49, and Ibid.
[60] For example, Article 10 of the European Convention on Human Rights states that everyone can hold their own opinions and obtain and communicate information and ideas without intervention from others. Various other states operate a similar concept, for example, the American Constitution.
[61] WIPO Case No. D2000-1015.
[62] Bally Total Fitness v. Faber, 29 Supp. 1161 (CD Cal 1998).
[63] Case D2002-0857.
[64] http://arbiter.wipo.int/domains/decisions/html/2002/d2002-0857.html, (Accessed 10/03/02).
[65] See further WHOIS Command overview, http://www.netsol.com/en_US/faq/whois/whois-learnmore.jhtml, (Accessed 10/03/02), (Accessed 10/03/02).
[66] Found at http://www.casdns.net/Help/FAQ/FAQ-WhoisInfo.htm, (Accessed 10/03/02).

[67] See further Directive (95/46/EC) of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the processing of Personal Data and the Free Movement of Such Data.
[68] See http://www.dataprotection.gov.uk/dpr/dpdoc.nsf/ed1e7ff5aa6def308025663600045bf4d/00cf047db319$FILE/8THPRIN.txt, (Accessed 10/03/02).
[69] See WHOIS and National Laws, http://lists.megacity.org/pipermail/spamfight-legal/2002-January/000024.html, (Accessed 10/03/02).
[70] See further Berman, Howard, L., House Judiciary Committee Subcommittee on Courts, the Internet and the Intellectual Property, *Oversight Hearing on The Whois Database: Privacy and Intellectual Property Issues*, July 12, 2001, http://www.house.gov/berman/int_prop071201.htm, , (Accessed 10/03/02).
[71] Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the Protection of Consumers in respect of Distance Contracts and Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal market.
[72] See further http://www.dnso.org/dnso/notes/20030219.WhoisTF-accuracy-and-bulkaccess.html, (Accessed 06/03/02).
[73] http://www.icannwatch.org/article.pl?sid=03/02/06/1347239&mode=thread, (Accessed 06/03/02)
[74] See further *New WHOIS*, http://www.namedropper.co.uk/Domains/Nominet_UK__The__uk_Registry_/Whois/whois.html.
[75] http://www.nominet.net/ref/whois3.html, (Accessed 12/02/02).
[76] *Supra* No. 40.