Cyber is understood as computer and mathematical analysis of the flow of information. The word ‘Cyber’ comes from the Greek word for navigator originating in kybernētē meaning ‘helmsman’. Cyberspace is the virtual (nonphysical) space created by computer systems that is, a shared virtual or metaphorical environment whose inhabitants, objects, and spaces comprise data that is visualized, heard and touched by surfing Internet. In other words, it is an artificial, virtual, conceptually constructed mental environment or notional space developed using computers. This very idyllic conception of imaginary locale which is not a land of utopia but a realm of experience was crafted by a futuristic designer author William Gibson who coined the term cyberspace in his ‘Burning Chrome’ in 1982 and later popularized by his sci-fi Hugo Award winning novel Neuromancer in 1984. The credit of Gibson had been acknowledged by John Perry Barlow in his works, ‘Crime and Puzzlement’ published in 1990. He writes, ‘In this silent world, all conversation is typed. To enter it, one forsakes both body and place and becomes a thing of words alone. You can see what your neighbours are saying (or recently said), but not what either they or their physical surroundings look like. Town meetings are continuous and discussions rage on everything from sexual kinks to depreciation schedules. Whether by one telephonic tendril or millions, they are all connected to one another. Collectively, they form what their inhabitants call the ‘Net’. It extends across that immense region of electron states, microwaves, magnetic fields, light pulses and thought which sci-fi writer William Gibson named Cyberspace.’ The problem is how to reconcile all the conflicting claims arising out of the issues of privacy in the context of Internet exposure vis-à-vis the right to freedom of speech. The paper will raise all these issues cropping up in a number of fields and discuss the legal implications on the encroachment of the freedom of speech.

**Keywords:** Cyber, freedom of speech, privacy, defamation, database

The route of the journey in the cyberspace is three-dimensional in so far as it is textual, audio and video electronic signals travel freely. Cyberspace is a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures. Various spatial metaphors related to cyberspace suffer from two main deficiencies. First, they do not take into account that cyberspace is not a pre-existent territory, but an entity that emerges in the process of its embryonic manifestation. Second, cyberspace is not a metric space, so that most of the ready-made constructs, like the topologic spaces, cannot be of much use.

Thanks to technological revolution, geography is now history. There has been a tectonic shift in modern life in the new millennium. Today, there are over 600 million people connected to the Internet worldwide. The Internet enables us to improve communication, erase physical barriers, and expand our education. Its absorption into our society has been extraordinary. The ‘Net’ touches nearly every part of our lives from how we search and apply for jobs and where we poke our nose for news, how we craft friendships. A few websites have virtually replaced the directory and dictionary.

There are five areas of privacy in the net: search and seizure, unsolicited e-mail, defamation, secrecy and the creation of databases consisting of personal information. All of these require legal protection while freedom of speech needs to remain unhindered.

**History of Internet**

In excitement and joy of invention by Samuel Morse of telegraphy, Nathaniel Hawthorne wrote in 1855: ‘By means of electricity, the world of matter has become a great nerve, vibrating thousands of miles in a breathless point of time ... The round globe is a vast ... brain, instinct with intelligence!’
Now, the tectonic shift introduced by Internet has revolutionized the computer and communications world like nothing before. The invention of the telegraph, telephone, radio, and computer set the stage for this unprecedented integration of capabilities. The Internet is at once a world-wide broadcasting capability, a mechanism for information dissemination, and a medium for collaboration and interaction between individuals and their computers without regard for geographic location. A fundamental pioneer in his clarion call for a global network, JCR Licklider, articulated the idea in his paper, Man-Computer Symbiosis (1960):

‘A network of such [computers], connected to one another by wide-band communication lines’ provided ‘the functions of present-day libraries together with anticipated advances in information storage and retrieval and [other] symbiotic functions’.

However, the term Internet has been used since 1974 and it was a tactical move originally designed in part to provide a communications networks that would work even if some of the sites were destroyed by nuclear attack. If the most direct route was not available, routers would direct traffic around the network via alternate routes. The story can be told by a narrative in post war scenario of nuclear winter in which the 'living will envy the dead' Controller to borrow Nikita Khrushchev’s words but an Adam may still be in search of an Eve or vice-versa for which communications would be more vital.

The statehood of a Republic of Cyberspace can be declared any moment the Government with its structure and functional sphere and authority is formed for Internet governance. Cyberspace has all the elements of a State like territory (space), inhabitants (netizens) and sovereignty (boundless domain protected by an army of soft wares against viral attack) but it is waiting for the supply of omission of governmental authority. ‘One planet-one Net’ campaign is already set on motion to cover management of Internet names and addresses, international policy issues relating to Internet governance and domain Names. The developed regulatory activity so far relates to defining protocols and standards.

Content Dynamics and Users’ Rights

In general, contents of Internet privacy need be encased to guarantee certain basic rights such as the following:

(i) Right to know: Users have a right to know what information relevant to themselves is collected by the websites, what purpose the information will be used, as well as who it will be shared with.

(ii) Right to choose: Consumers have a right to choose the use of their personal data.

(iii) Right to reasonable access: Consumers have the right to access the personal data and amend or delete the wrong information through reasonable approaches in order to ensure that the personal information is accurate and complete.

(iv) Right to adequate security: The network company should guarantee the security of users’ information and prevent unauthorized illegal access. The users have the right to request the website to take the necessary and reasonable measures to protect their personal information.

In addition, Internet privacy should also include the user’s right to control the information (the user has the right to decide whether to allow others to collect or use his information) and the right to access judicial relief (the user has the right to bring a civil suit against any institution or individual engaged in infringement on his privacy).

Yahoo’s Internet Privacy Policy

Cyberspace privacy of personal information mainly refers to the right of citizens to enjoy the network’s private life with peace of mind and the protection of private information in accordance with the law. Privacy stipulates that personal information including facts and images should not be unlawfully infringed, known, collected, copied, disclosed, transferred or utilized by others. Circulation of personal information may play havoc because of its distortion, misuse and wanton exploitation. Yahoo has devised its privacy policy based on the principle of restricted use of personal information on permissive basis. As a rule, Yahoo does not rent, sell or share personal information except on permission or under limited circumstances when it has to work with trusted partners under confidentiality agreement and they are legally required to respond to court’s subpoena, orders or legal process to establish and exercise legal rights and defend against legal claims. These information also may have to be shared or divulged in the interest of investigation, prevention and remedial actions against illegal activities, suspected fraud, potential threat to the physical safety...
of any person, violation of terms of use or as required by law and also when merger and acquisition process are ensued but with prior notification. These are very reasonable grounds on which privacy issue necessarily takes a back seat.

Country Context

Concerns about access to content on the Internet vary markedly in different countries around the world and regulatory mechanism and policy reflect this. What is illegal in one country is not illegal in others, and what is deemed unsuitable for minors in one country is not unsuitable in others. Films classified R18 in Australia are often classified suitable for persons under 18 years in other countries, e.g. Intimacy (sex scenes) and Hannibal (violence) are classified 18 in Australia, but are classified 12 in France. However, France prohibits the display of Nazi memorabilia, including on web pages, which is not prohibited by Australian offline laws or by existing or proposed online censorship laws. Many similar examples demonstrate the weak biting capacity of national censorship laws to protect children (or adults) on the Internet.

The USA is not the only country where citizens have the pinnacle of a right to freedom of expression. In contrast to Australia, governments in comparable countries including Canada, New Zealand, the United Kingdom and various European countries have chosen to legislate to give citizens a right in domestic law to freedom of expression similar to that contained in the International Convention on Civil and Political Rights (ICCPR). Such a right is by no means absolute and does not prevent governments from enacting or enforcing laws restricting freedom of expression. However, governments in these countries have not enacted or indicated any intent to enact, Internet censorship legislation as restrictive of adults’ freedom of expression, as that existing and proposed in Australia.

China

Article 38 of the Constitution provides that the human dignity of citizens should not be infringed. Article 39 provides that the premises should not be trespassed. Article 40 stipulates that the freedom and privacy of correspondence of citizens are protected by law. These are parts of the privacy of citizens and general principles set out by the Constitution as the basic law. Being not practical and inclusive, these provisions only provide the basis for the protection of privacy by other supplemental laws and regulations.

Legal Protection

Article 7 of the Measures for Security Protection Administration of the International Networking of Computer Information Networks in the Peoples’ Republic of China (PRC) provides that users’ freedom of communication and communications secrecy is protected by law. No unit or individual shall use the international networking to infringe on users’ freedom of communication and communications secrecy in violation of the provisions of law. Article 18 of the Implementation Rules for Provisional Regulations of the Administration of International Networking of Computer Information in the PRC provides that it is prohibited to infringe on the privacy of others by accessing computer systems without authorization, tampering with the information of others or sending information in the name of others. However, these provisions are too broad to be applied in legal practice. The right of privacy is to great extent secured by Internet censorship curtailing the potential of infringement which is indicative of the limited freedom of speech enjoyed by the people. Internet censorship in the PRC has been called a panopticon that encourages self-censorship through the perception that users are being watched.

Definition

On 24 October 1995, the Federal Networking Council (FNC) unanimously passed a resolution defining the term ‘Internet’. This definition was developed in consultation with members of the Internet and intellectual property rights communities.

Resolution: The FNC agrees that the following language reflects our definition of the term ‘Internet’: ‘Internet’ refers to the global information system that -- (i) is logically linked together by a globally unique address space based on the Internet Protocol (IP) or its subsequent extensions/follow-ons; (ii) is able to support communications using the Transmission Control Protocol/Internet Protocol (TCP/IP) suite or its subsequent extensions/follow-ons, and/or other IP-compatible protocols; and (iii) provides, uses or makes accessible, either publicly or privately, high level services layered on the communications and related infrastructure described herein.
Privacy and Freedom of Speech

Privacy

Privacy is highly prized by many people. In essence, it is a debate about the control of personal information. It is not much about massive means of electromagnetic monitoring rather its use or misuse which can be exchanged, bought or sold for secondary use without one’s knowledge or consent. Privacy is viewed as a precious protective personal possession against paparazzi and peeping Toms of various outfits even though ‘no man is an island, entire of itself;’ ‘….'

In ultimate analysis, privacy choices are individual, anything else is an automatic invasion of one’s privacy. Privacy might be considered an ‘inalienable right’, either protected by the constitution of a country although in fact may not be directly addressed or by ordinary law of the land. On the other hand, self-defence is a right which supersedes virtually all rights, constitutions, statutes, and rules. Privacy is logically and rationally tied to self-defence. The Fifth Amendment of US Constitution which limits self-incrimination also projects an aspect of privacy in protective gear. At the same time, privacy is required to be sacrificed for safety and security reasons and no one objects to such arrangement in general.

Simply stated, privacy means it is the right to ‘be let alone’. This classical definition is too simplistic and it obviously cannot serve today’s world of interconnectivity. Privacy is the ability of an individual or group to keep their lives and personal affairs out of public view, or to control the flow of information about themselves. Construed differently, privacy is the ability of an individual or organization to reveal oneself consciously and selectively. Privacy is sometimes related to anonymity although it is often most highly valued by people who are publicly known. Privacy can be seen as an aspect of security — one in which trade-offs between the interests of one group and another can become particularly clear. The words ‘private’ and ‘privacy’ can be construed accordingly.

The confidentiality, integrity, and availability of data and networks -- including critical infrastructure -- is central to attracting FDI and IT operations to developing countries. On the other hand, it is equally important to safeguard privacy of the individual arising out of human ‘dignitas’ a right recognized by Article 12 of the United Nations Declaration on Human Rights, 1948, which says, ‘No one shall be subjected to arbitrary interference with his privacy, family, home and correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of law against such interference or attacks.’

Article 17 of ICCPR and Article 8 of ECHR similarly seek to protect the right of privacy. The question of privacy can be viewed from four angles given the fact that it arises out of the principle of dignitas, namely, ‘person’, ‘property and possessions’ to remain free from intrusion, ‘seizure’ and ‘personal communications’ protected from interference and disclosure.

The right against unsanctioned invasion of privacy by the government, corporations or individuals is part of many countries’ privacy law, and in some cases, constitutions. Almost all countries have laws which in some way limit privacy; an example of this would be law concerning taxation, which normally requires the sharing of information about personal income or earnings. In some countries, individual privacy may conflict with freedom of speech laws and some laws may require public disclosure of information which would be considered private in other countries and cultures. The law of privacy is the weakest in the United Kingdom. Lord Scarman maintained in R v IRC ex parte Rossminster Ltd2 that Taxes Management Act, 1970 provided amplitude of power amounting to ‘a breath-taking inroad upon the individual’s right of privacy and right of property’ and yet allowed its breadth since parliament had created the power and it had been lawfully exercised. In the case of Malone v Metropolitan Police Commissioner [No. 2]3 the Court rejected the argument that the tapping of Malone’s telephone in the course of a criminal investigation violated his right of privacy. In fact, there is no recognized right to privacy under the law of England. In Ireland, the Judge took a different stand in Kennedy v Ireland [(1987)]4 although there was no specific right to privacy, the Court relied upon the provisions of Article 40(3) of the Constitution which inter alia provided for the guarantee to vindicate personal rights of the citizens. In Griswold v Connecticut5 Court found that there were ‘penumbras formed by the emanations from’ the First, Third, Fourth, Fifth, Ninth, and Fourteenth Amendment guarantee that created a zone of privacy in the US.

In the new information and communication age of the Internet, there is serious and growing threat to right of privacy. The oft-quoted passage of Alexander Solzhenitsyn from his Cancer Ward (1968) is quite enlightening statement:

---
‘As every man goes through life he fills in a number of forms for the records, each containing a number of questions... There are thus hundreds of little threads radiating from every man, millions of threads in all. If all these threads were suddenly to become visible, the whole would look like a spider’s web, and if they materialized as rubbers, bands, buses, trams and even people would lose ability to move... They are not visible, they are not material but everyman is aware of their existence... Each man permanently aware of his own invisible threads naturally develops a respect for the people who manipulate the threads.’

The variety of technological marvels introduced on daily basis is so innovative that one has to constantly keep track and monitor those irritant and damaging devices and techniques in order to protect against invasion of privacy and apparently there is no fool-proof immunity against this tide. Thus, cookies are not merely baked products from the bakery for munching any more, they also are pieces of information or small files that a website can send to your computer’s hard drive for record keeping. Cookies can make using websites easier to use by storing information about your preferences on a particular website. The information may remain on your computer after the Internet session finishes. While the main website does not use cookies, cookies may be sent by the department’s online applications accessed via the main website. Webmasters have begun using ‘cookies’ as a means of accumulating information about web surfers without having to ask for it. Cookies attempt to keep track of visitors to a website. Critical analysis of cookies has apprehended the fear of the loss of privacy. The information that cookies collect from users may be profitable both in the aggregate and by the individual. Whether the convenience that cookies provide outweighs the loss of privacy is a question each Internet user must decide for himself or herself.

Surveillance
‘Every step you take/every move you make/every vow you break/I’ll be watching you’ is not exactly musical but can be a real sting. Nordic Conference of Jurists and Legal Experts (31 Bulletin of the International Commission of Jurists, September, 1967, 1-11,) emphasized that right to privacy is of paramount importance for human happiness.

English Jurisdiction
Sara Cox and her new husband, Jon Carter, were photographed naked on their honeymoon in a private island in the Seychelles in October 2001. The pictures were taken without their knowledge, while they were at their own villa, by a paparazzi photographer in another villa. The week after publication ‘The People’ apologized - part of a deal brokered by the Press Complaints Commission. Nonetheless, Cox and her husband went ahead and sued, under Article 8 of the European Convention of Human Rights which guarantees, ‘everyone has the right to respect for his private and family life, his home and his correspondence’. After many months the newspaper has settled out of court, agreed to pay the couple’s costs (a sum over £100,000) and destroyed the pictures.

Law of Confidence
Catherine Zeta-Jones and Michael Douglas won their case against ‘Hello’ magazine over unauthorized photographs of their wedding - but not because their privacy had been invaded. The couple won because their £1m exclusive deal with rival magazine ‘OK’ meant pictures of their wedding were in effect a trade secret, and so protected under the law of confidence.

Unauthorized Photographs on the Internet and Ancillary Privacy Issues
Internet users are among the world’s most closely observed specimens of humanity. Consultants and marketing experts scrutinize them, monitor their desires and anticipate their reactions, for they know the future of the information economy. In the summer of 1998, a case involving chat room privacy arose in the Ontario Court (General Division). Yahoo was operating a discussion group and a number of anonymous participants posted allegedly defamatory messages through Yahoo’s facility. Phillips Services Corp, a Canadian public company, applied to the Court ex parte (without giving any advance notice to anyone of the Court hearing) and the Court was persuaded to order that a number of ISPs identify the names, addressed and other particulars of the persons who had posted the messages. At the time, commentators opined that the orders ‘illustrate that the judicial system is not about to let the Internet operate in a legal vacuum. They confirm – if in fact there was any doubt – that the general laws apply in cyberspace as well.’ Unlike other forms of discussion like a newspaper’s letter-to-the-editor section, the
The instantaneous nature of cyberspace does not typically involve ISPs editing content for, among other things, defamatory statements. But it appears, based on the Phillips Services Corp case, that the author will, nonetheless, be held accountable by Canadian courts.

**Basic Consumer Privacy Protection**

The ILO’s Code of Practice on the protection of workers’ personal data in technological era issued a set of principles in 1997 aiming to secure fundamental right to privacy. The general principles of the code are:

(i) Personal data should be used lawfully and fairly; only for reasons directly relevant to the employment of the worker and only for the purposes for which they were originally collected;

(ii) Employers should not collect sensitive personal data (e.g., concerning a worker's sex life; political, religious, or other beliefs; or trade union membership or criminal convictions) unless that information is directly relevant to an employment decision and is collected in conformity with national legislation;

(iii) Polygraphs, truth-verification equipment or any other similar testing procedure should not be used;

(iv) Medical data should only be collected in conformity with national legislation and principles of medical confidentiality; genetic screening should be prohibited or limited to cases explicitly authorized by national legislation; and drug testing should only be undertaken in conformity with national law and practice or international standards;

(v) Workers should be informed in advance of any monitoring, and any data collected by such monitoring should not be the only factors in evaluating performance;

(vi) Employers should ensure the security of personal data against loss, unauthorized access, use, alteration or disclosure; and

(vii) Employees should be informed regularly of any data held about them and be given access to that data.

The Code does not form international law and is not of binding effect. It was intended to be used ‘in the development of legislation, regulations, collective agreements, work rules, policies and practical measures’. Unfortunately, however, the laws differ greatly from country to country, and in some countries there are few legal constraints on workplace surveillance. The French Supreme Court held that employers do not have the right to open any of their employees’ messages. The Court ruled in a case between Nikon and a former employee that the company had no automatic right to search through an e-mail inbox. European system of data protection initially covered only personal information stored in computerized form and had been extended to cover organized collection of manually accessible information. The Privacy and Electronic Communications (EC Directive) Regulations, 2003 w.e.f. 11 December 2003 further tightened and strengthened. Applying to the federal sector, Electronic Communications Privacy Act, 1986 has been diluted by the Patriot Act in the United States.

**Reasonable Expectation**

In *Gary Leventhal v Lawrence Knapek* the Second Circuit held that a government employee has a reasonable expectation of privacy in an office computer located in his private office in the light of the absence of both a computer usage policy advising him to the contrary, and a regular practice by his employer of searching the same. The Court nonetheless held that the government’s search of its employee’s computer for evidence of suspected work-related misconduct did not violate the employee’s rights under the Fourth Amendment. Such searches are permitted if the search is both justified at its inception and of appropriate scope. Such was the case in the instant matter because the government had received notice of alleged job-related misconduct by the plaintiff employee and had conducted an appropriately circumspect inspection of his office computer to ascertain the validity of these allegations. In *R v Edwards*, the Canadian approach revealed a different line of thought and arguably the law protected privacy of people and not places in this context. In the business world a different a different principle is applied. Thus, in *TBG Ins Services Corp v Robert Zieminski* a computer usage policy by which a company retains its right to inspect computers provided to employee for business use entitles the company to inspect the contents of its computer used by the employee in his home in spite of objections once the employee consented to such policy by agreement pursuant to the policy. In this case, the Court observed, ‘[Company’s] advance notice to
[Employee](the company’s policy statement) gave [Employee] the opportunity to consent to or reject the very thing that he now complains about, and that notice, combined with his written consent to the policy, defeats[the] claim that he had a reasonable expectation of privacy.

In *Apple v Doe 1, et al.* the Court denied bloggers’ motion for a protective order, which sought to quash a subpoena served by Apple Computer Inc (Apple) on Nfox, the e-mail service provider for the blog PowerPage. The subpoena, inter alia, sought materials, including e-mails that would permit Apple to identify the individual(s) who transmitted trade secret information about an Apple product to PowerPage, which information PowerPage subsequently published on its blog/website. The Court held that the bloggers were not entitled to such relief under California’s ‘Shield law’, since that statute only protects journalists from being found in contempt for failing to produce information, which was unsupportive of the motion to quash. Trading in trade secret is an indulgence in criminal activity and cannot enjoy the fruits of privilege extended to journalists under the First Amendment. Since Apple had proved a *prima facie* case that a crime had been committed, it was entitled to the discovery.

In *Bidzirk LLC et al. v Philip J Smith* granting defendant’s motion for summary judgment, the District Court dismissed defamation, trademark infringement and invasion of privacy claims brought by plaintiffs against a blogger. The claims were rooted in defendant’s publication of articles on his blog, featuring plaintiff’s trademark that were critical of eBay auction listing business. The Court held that plaintiff’s trademark dilution claims could not succeed because the defendant used the mark in connection with ‘news reporting and news commentary,’ a non-actionable use under Federal Dilution Statute. Plaintiff’s defamation claims also failed because the statements at issue— which purportedly accused plaintiff Schmidt of being a ‘yes man’ ‘who over-promised and under-delivered’ were non-actionable statements of opinion. Plaintiff’s invasion of privacy claims – which were premised on a link on defendant’s blog to another site which displayed a picture of the plaintiff also failed. The Court rested the decision on its determination on the ground that both South Carolina law did not recognise a claim for false light invasion of privacy, and that, in any event, the link and article in question did not project the plaintiff in a false light. The Court also grounded its rejection of privacy claim by finding that the link and corresponding use of the photo did not constitute a viable ‘wrongful appropriation of personality’s invasion of privacy, given that plaintiff had consented to the use of their photo on the Internet site on which it was contained.

It is possible to infringe a person’s privacy right by creating e-mail Id/Account in that person’s name as decided by the Indiana Supreme in *University of Evansville v Dr. William Felsher.*

**Defamation**

‘Good name in man and woman, dear my lord, Is the immediate jewel of their souls: Who steals my purse, steals trash; `t is something, nothing; T was mine, `t is his, and has been slave to thousands; But he that filches from me my good name Robs me of that which not enriches him And makes me poor indeed.’

The immediate jewels of our souls are in stake in this digital age. Hence, defamatory statement and defamatory sense are both to be counted in the process of dissemination of information through the new space filled by the sometimes anonymous intruders and perpetrators. The basic framework of defamation law has not changed much although there are changes taking place, since honour and reputation are valued in most jurisdictions around the world. The classic definition in *Sim v Stretch* still forms the basis of defining what constitutes defamation. In general, Lord Atkin said, there is no satisfactory definition. The traditional view, that a defamation is something that exposes the victim to ‘hatred, ridicule, or contempt’, was too narrow, and he preferred the view that a defamation is something that "tends to lower the claimant in the estimation of right-thinking members of society".

Let us examine the law in this course in the light of the dissemination and communication taking place in some prominent jurisdictional spheres.

**United States**

In *Mark Andrew Austin v Crystaltech Web Hosting, et al.* the Court held that the Communications Decency Act, 1996 immunizes web hosting company from liability arising out of its hosting of a third party’s website that allegedly contained defamatory statements about the plaintiff. In line with the Fourth
Circuit’s decision in Zeran v AOL\textsuperscript{17} the Court maintained that such immunity exists notwithstanding any notice the web hosting company received concerning the defamatory nature of the content it was hosting. The Court also dismissed defamation claims against the originator of the content on the ground of lacking personal jurisdiction over the defendant in spite of the fact that the defendant had contracted with an Arizona web hosting company to host the website which published the defamatory statements at issue. The Court reasoned that the exercise of jurisdiction over the defendant would be unreasonable given the fact that he was a non-resident, the parties each operated Bali-related travel services, and the dispute was governed by Bali law.

In Cecilia Barnes v Yahoo Inc\textsuperscript{18}, also the Court held that the Communication Decency Act immunizes Yahoo, Inc (Yahoo) from tort claims arising out of its alleged failure to timely honour promises to remove from Yahoo’s website objectionable contents about the plaintiff posted by a third party. The contents profiled nude photos of plaintiff and accurate contact information.

There is an increasing trend among companies to dismiss or sue employees for divulging company ‘trade secrets’ or defaming the company in chat rooms. These have become known as ‘John Doe’ cases. Because most people log on to chat rooms anonymously or use an alias, once a company observes a certain party in a chat room engaging in ‘illegitimate’ speech, they must subpoena the message-board services such as Yahoo! or America Online, it then obtains the identity of the specific author. The service providers often turn over identifying information when presented with a subpoena without any notice to the individual. The number of these cases is rapidly increasing and threatens not only the privacy of employees but also their rights to anonymity and free speech.

In some cases, companies have asked the Court to identify the authors of anonymous defamatory messages. This has been done by filing ‘John Doe’ lawsuits and issuing subpoenas to Yahoo! and other message boards where individuals have posted the disparaging messages. Journalists can also face problems although claim that they only report news and do not create any, in view of the new judgments emerging from the commonwealth jurisdictions.

Jurisdictional Issue in the US

The enactment of the Communications Decency Act of 1996 has made US cyber law even more permissive. That Act gives commercial interactive computer service providers immunity from liability for material posted by third parties. However, the Act had been declared as unconstitutional. The California Supreme Court held, in Barrett v Rosenthal\textsuperscript{19}, that Internet users who post (to Web sites or discussion groups) material created by others are immune from liability. While Congress could have made a different policy choice, it opted not to hold interactive computer services liable for their failure to edit, withhold or restrict access to offensive material disseminated through their medium Section 230(c) [of the Communications Decency Act of 1996] provides:

‘No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.’

AOL was nothing more than a provider of an interactive computer service on which the Drudge Report was carried, and Congress has said quite clearly that such a provider shall not be treated as a ‘publisher or speaker’ and therefore may not be held liable in tort.

In Blumenthal v Drudge\textsuperscript{20} case Matt Drudge (who, as author, could not claim immunity under the Act) applied to the US District Court for the District of Columbia for a motion to dismiss or transfer the case for want of personal jurisdiction over him (a resident of California). The decision turns on the ‘long arm’ statute of the District of Columbia, but many states and provinces have similar legislation. The Court stated: The legal questions surrounding the exercise of personal jurisdiction in ‘cyberspace’ are relatively new, and different courts have reached different conclusions as to how far their jurisdiction extends in cases involving the Internet. Generally, the debate over jurisdiction in cyberspace has revolved around two issues: passive web sites versus interactive web sites, and whether a defendant’s Internet-related contacts with the forum combined with other non-Internet related contracts are sufficient to establish a persistent course of conduct.

At one end of the spectrum are situations where a defendant clearly does business over the Internet. If the defendant enters into contracts with residents of a foreign jurisdiction that involve the knowing and repeated transmission of computer files over the Internet, personal jurisdiction is proper. At the other end are situations where a defendant has simply posted information on an Internet website which is
accessible to users in foreign jurisdictions. A passive website that does little more than make information available to those who are interested in it, is not grounds for the exercise [of] personal jurisdiction. The middle ground is occupied by interactive websites where a user can exchange information with the host computer. Surely, in these cases, the exercise of jurisdiction is determined by examining the level of interactivity and commercial nature of the exchange of information that occurs on the website (Zippo Mfg Co v Zippo Dot Com Inc).

Drudge and his counsel attempted to label the Drudge Report as a ‘passive’ website; the Court found this characterization inept. The Drudge Report’s website allowed browsers, including District of Columbia residents, to directly e-mail defendant Drudge, thus allowing an exchange of information between the browser’s computer and Drudge’s host computer. The constant exchange of information and direct communication that District of Columbia Internet users are able to have with Drudge’s host computer via his website is the epitome of website interactivity. Even though Drudge may not advertise in . . . local newspapers in Washington, DC, the subject matter of the Drudge Report is directly related to the political world of the Nation’s capital and is quintessentially ‘inside the Beltway’ gossip and rumor. . . . Drudge’s motion to dismiss or transfer for want of personal jurisdiction, therefore, was denied.

In case of Edias Software Intern v Basis Intern Ltd, the plaintiff brought an action against the defendant for breach of contract, libel, defamation, tortuous interference with contract and prospective advantage, and violation of the US Lanham Act. The defendant sought an order dismissing the action for lack of jurisdiction. The defamation portion of the claim revolved around allegations that the defendant posted defamatory e-mail messages to its customers about its contract dispute with the plaintiff, and issued a ‘press release’ on its CompuServe Webpage and in a computer forum. Citing the US Supreme Court case of Calder v Jones the Arizona Court confirmed that libelous statements by a non-resident can form the basis for jurisdiction in the plaintiff’s forum. The Court concluded that the e-mail, Webpage and forum message were directed at Arizona and allegedly caused foreseeable harm to the plaintiff. The defendant’s application was dismissed. This case is a departure, rather a u-turn from the principle stated in Mark Andrew Austin v Crystaltech Web Hosting, et al. In Heroes, Inc v Heroes Foundation, the District Court for the District of Columbia found jurisdiction in circumstances where the defendant had an Internet homepage that solicited donations and provided a toll-free telephone number for donors.

In Inset Systems, Inc v Instruction Set, Inc, the plaintiff, a Connecticut company, brought a trademark infringement action against the defendant, a Massachusetts company, in Connecticut. The defendant applied for an order dismissing the action for lack of personal jurisdiction and improper venue. The Court dismissed the motion, holding that the defendant’s advertising via the Internet was solicitation of sufficient repetitive nature to satisfy the ‘solicitation of business’ provision of the Connecticut long-arm statute. Although it appears that the decision found jurisdiction solely on the basis of the defendant’s Internet presence the Court may have been influenced by the fact the defendant also had a toll-free number included in its website. In finding jurisdiction the Court said [p. 165]:

‘In the present case, Instruction has directed its advertising activities via the Internet and its toll-free number toward not only the state of Connecticut, but to all states. The Internet and toll-free numbers are designed to communicate with people and their businesses in every state. Advertisement on the Internet can reach as many as 10,000 Internet users within Connecticut alone. Further, once posted on the Internet, unlike television and radio advertising, the advertisement is available continuously to any Internet user. ISI has therefore, purposefully availed itself of the privilege of doing business within Connecticut’.

In case of Smith v Lobby Shops, the defendant retailer third-partied the Hong Kong manufacturer of an artificial Christmas tree that allegedly caused a fatal house fire. The third party applied to dismiss for lack of personal jurisdiction. The Court granted the motion concluding that the third party’s advertisement in a trade publication that appeared on the Internet was insufficient ‘contact’ with the jurisdiction to support hauling it into court.

Yet, in case of Weber v Jolly Hotels, the Court held that an Italian Corporation’s use of an Internet computer network to advertise its hotels in Italy did not amount, on its own, to a purposeful adoption of New Jersey law for the purposes of determining
jurisdiction. The plaintiff, a New Jersey resident, was injured while vacationing at one of the defendant’s hotels in Italy. The Court concluded [p. 334] that ‘advertising on the Internet is not tantamount to directing activity at or to purposefully availing oneself of a particular forum.’

In CompuServe, Inc v Patterson, the plaintiff company sought a declaration that it had not infringed the defendant’s common-law trademarks or otherwise engaged in unfair competition in respect of computer software developed by the defendant. The Sixth Circuit Court of Appeals reversed a Lower Court decision which had dismissed the action for lack of personal jurisdiction. In reaching its conclusions the Court found that the defendant had purposely availed himself of benefits of doing business in the plaintiff’s home state and that the action arose from the defendant’s contacts with the state in question, in this case Ohio. The defendant had placed software exclusively on the plaintiff’s website, had used the website to sell and advertise his software, and had threatened, via e-mail messages sent to Ohio, to seek an injunction and damages against the plaintiff regarding its sales of his software if the plaintiff failed to comply with his demands. The Court said [p. 1264]:

‘There is no question that Patterson himself took actions that created a connection with Ohio in the instant case. He subscribed to CompuServe, and then he entered into the Shareware Registration Agreement when he loaded his software onto the CompuServe system for others to use and, perhaps, purchase. Once Patterson had done those two things, he was on notice that he had made contracts, to be governed by Ohio law, with an Ohio-based company. Then, he repeatedly sent his computer software, via electronic links, to the CompuServe system in Ohio, and he advertised that software on the CompuServe system. Moreover, he initiated the events that led to the filing of this suit by making demands of CompuServe via electronic and regular mail messages’.

In Maritz, Inc v Cybergold, Inc, a trademark infringement action, the Missouri District Court found it had jurisdiction over a California operator of an Internet site that maintained a mailing list of Internet users for advertising, knew that its information would be transmitted globally, had transmitted information into Missouri over a hundred times, and allegedly caused economic injury to a Missouri corporation. The defendant’s website provided information about the defendant’s service, which, at the time, was not operational. The service was designed to provide subscribers with information in the form of advertisements based on the subscribers particular interests. The information would be posted to a mailbox set up for each subscriber. The Court concluded, among other things, that the defendant had . . . obtained the website for the purpose of, and in anticipation that, Internet users, searching the Internet for websites, will access CyberGold’s website and eventually sign up on CyberGold’s mailing list. Although CyberGold characterizes its activity as merely maintaining a ‘passive website,’ its intent is to reach all Internet users, regardless of geographic location, [p. 1333]. As a result, the Court concluded [p. 1334] that the defendant ‘through its Internet activities, has purposely availed itself of the privilege of doing business with this forum such that it could reasonably anticipate the possibility of being hauled into court here.’

Similar to the Inset Systems case, Maritz case suggests that merely having a website presence accessible in a particular state may result in jurisdiction being found. By contrast, the New York District Court in case of Bensusan Restaurant Corp v King, held that the mere fact that Internet users can gain information about a person or company from an Internet site is not necessarily the equivalent of that person or company advertising, promoting, selling or otherwise making an effort to do business in a particular state. The Court concluded that there must be something more to establish that a party is directing activities towards that particular jurisdiction. In Bensusan, the Court found that the defendant, a Missouri company, had set up a website with a Missouri telephone number posted so that people could order tickets to attend shows at the defendant’s nightclub in Missouri. The nightclub had the same name as a New York nightclub owned by the plaintiff. The plaintiff sued, but the Court dismissed the action on the basis of lack of jurisdiction. The Court said that the mere setting up of the website with a Missouri telephone number did not amount to an offer by the defendant to sell products in New York. In this case, there was no allegation that any infringing products (i.e., tickets) were shipped to New York or that any other infringing activity was directed at New York.

The case of Zippo Mfg Co v Zippo Dot Com, Inc, cited earlier the Court established a sliding scale for
determining jurisdiction in cases involving the Internet. The Court said [pp 1123-1124] that

‘... (t)he Internet makes it possible to conduct business throughout the world entirely from a desktop. With this global revolution looming on the horizon, the development of the law concerning the permissible scope of personal jurisdiction based on Internet use is in its infant stages. The cases are scant. Nevertheless, our review of the available cases and materials reveals that the likelihood that personal jurisdiction can be constitutionally exercised is directly proportionate to the nature and quality of commercial activity that an entity conducts over the Internet. This sliding scale is consistent with well developed personal jurisdiction principles. At one end of the spectrum are situations where a defendant clearly does business over the Internet. If the defendant enters into contract with residents of a foreign jurisdiction that involves the knowing and repeated transmission of computer files over the Internet, invocation of personal jurisdiction is proper (e.g. CompuServe Inc v Patterson). At the opposite end are situations where a defendant has simply posted information on an Internet website which is accessible to users in foreign jurisdictions. A passive website that does little more than make information available to those who are interested in it is not grounds for the exercise of personal jurisdiction. The middle ground is occupied by interactive websites where a user can exchange information with the host computer. In these cases, the exercise of jurisdiction is determined by examining the level of interactivity and commercial nature of the exchange of information that occurs on the website. (e.g. Maritz, Inc v Cybergold Inc). In Zippo, the Court found jurisdiction on the basis that the defendant online computer news service purposefully availed itself of doing business in Pennsylvania by operating an Internet site to advertise and solicit customers for its service and by entering contracts with thousands of individuals and seven access providers in Pennsylvania for the purpose of providing those individuals with its service.

The case of Cybersell, Inc v Cybersell, Inc (decided after Zippo) an Arizona corporation that advertised for commercial services over the Internet (the plaintiff) brought an infringement action against a Florida corporation (the defendant). The defendant sought to dismiss for lack of jurisdiction. The Court of Appeal upheld a Lower Court’s dismissal of the action on the grounds that the defendant’s use of the name ‘Cybersell’ in a passive home page on the world wide web was not enough to support the conclusion that it had purposefully availed itself of the privilege of doing business in Arizona and thus was not subject to personal jurisdiction in Arizona.

In Telco Communications v An Apple A Day, the Virginia District Court had to deal with an defamation action brought by a seller of long-distance services against a telemarketer. The defendant telemarketer had posted allegedly defamatory press releases regarding the plaintiff company on a passive Internet site. The defendant had also provided a telephone number at which he could be contacted. The press release also included a solicitation for business. The Court dismissed the defendant’s application to dismiss for lack of personal jurisdiction on the grounds that the defendant knew the press releases would be disseminated in Virginia. In reaching its decision the Court referred to Inset Systems for the proposition that a continuous Website constituted the purposeful doing of business in the state [p. 406]. The Court also referred to Bensusan and Zippo.

In case of Mallinckrodt Medical v Sonus Pharmaceuticals, the plaintiff sought a declaration that patents relating to a certain product were invalid and, further, that one of the defendants had made false and defamatory statements regarding the plaintiff. Several of the defendants moved to dismiss, including the defendant alleged to have made the defamatory statements. In dismissing the plaintiff’s action in respect of the defamation allegation, the Court concluded there is no nationwide jurisdiction for defamation actions. It stated [p. 272]:

‘The AOL transmission from Seattle to Virginia, which was subsequently posted on an AOL electronic bulletin board and may have been accessed by AOL subscribers in the District of Columbia, can not be construed as ‘transacting business’ in the District of Columbia. The message was not sent to or from the District of Columbia, the subject matter of the message had nothing to do with the District of Columbia, and neither plaintiffs nor Sonus reside in, have their headquarters in or are incorporated in the District. Other than the fact that some people may
have visited the electronic bulletin board and read the message from here, the AOL posting has no connection to this jurisdiction. The act of posting a message on an AOL electronic bulletin board - which certain AOL subscribers may or may not choose to access, according to each individual's tastes and interests - is not an act purposefully or foreseeably aimed at the District of Columbia".

**Conclusion**

Giving up privacy, freedoms, or rights for some perceived benefit is an individual choice. The key is whether or not the choice to give up privacy is an informed, voluntary, and willful one. While the voluntary aspect is strongly dependent upon the specifics of the lack of privacy or gained benefit scenario, being informed is generally less difficult, and is perhaps the first step. Freedom of speech has always been restricted although in some countries say, in the United States it is optimum but that sometimes can derail the process of integration. Thus, outrageous incidents like burning national flag as an expression of symbolic speech of protest can undermine national honour and take place paralysing the pride of freedom itself. The wisdom is in restraint and restrictions which are reasonable in all circumstances in order to serve the interest of privacy for the sake of similar protection of the invader of privacy himself.

It is clear that only home country regulation can effectively combat the menace of invasion of privacy as introduced in Australia in order to rein in the megaphone of Internet users who publish information or control personal data. Both privacy and freedom of speech are important and one cannot be jettisoned for the sake of the other. The conflicts can be managed by due process of law provided, law is found and the balance can be struck and maintained if a reasonable approach to respect and protect each of these rights is adopted at both national and international level. It is assuming more importance that a consensus on minimum level of restrictions on free speech be devised in an acceptable manner so as to pursue the common goal by introduction of home country regulation. The risk run by all parties can be reduced substantially by addressing the conflicting issues in a balanced approach.

**References**

1. John Donne’s Meditation 17 from Devotion upon Emergent Occasions (1624).
3. [1979] 2All ER 620.
4. IR 587.
5. 381 US 479 (1965).
7. Directive 95/45/EC.
8. 266 F3d 64(2d Cir, 26 September 2001), United States of America v Eric Neil Angevine 281 F3d 1130 (10th Circuit, 22 February 2002), 537 US 845(2002) in which it was held that a University Professor has no reasonable expectation of privacy in the face of a computer policy supportive of inspection.
10. 96 Cal App 4th 443 (Cal Ct App 2002) 446.
13. No.82 S04-0008-CV-477(Sup Crt Ind, 1 October 2001).
15. [1936] All ER 1237 (HL).
16. 1 CA-CV 04-0823, 125 P 3d 389 (Arz Crt App, 2006).
18. CIV No. 05-926-AA(D Or, 8 November 2005).
22. 947 F Supp 413 (D Ariz).
24. 1 CA-CV 04-0823, 125 P 3d 389 (Arz Crt App, 2006).
27. 968 F Supp 1356, 1365 (W D Ark1997).
29. 29 89 F 3d 1257, 39 USPQ 2d (BNA) 1502 (6th Cir 1996).
31. 126 F 3d 25, 44 USPQ 2d (BNA) 1051 (2nd Cir 1997).
32. 952 F Supp 1119 (ED Penn, 16 January 1997).