1. Introduction

Internet introduces facilities one could not imagine before. This technology was meant to ease military and computer scientist to communicate. It was developed within framework “if world war III is going to break out this technique shall reroute messages over different set of wires from one computer to another if anything went wrong between them; say a wire or computer got zapped by a nuclear blast in one place, the message could be sent by way of other place. Internet, as it is today, offers access to a vast amount of information. It lets a person communicate in so many ways with so many people wherever they be, down the street or on the other side of the globe. It gives its user the power over the way he shops, lives, works and even the way one has fun. It’s the greatest information-gathering resources ever invented – but that also means it is an easy way to gather information about a person. In spite the advantages Internet can offer, there has been an emerging call for protection of privacy over the Internet.

The word “privacy” is not easy to define. It’s very much connected with someone’s liberty to do something without interference of others. Judith Wagner (1997) highlighted that privacy may refer to the separation of spheres of activity, limits on governmental authority, forbidden knowledge and experience, limited access, and ideas of group membership, etc.[1] Invasions of privacy on the Internet may occur in so many ways. In January 1999, Scott McNealy, the chief executive officer of Sun Microsystems, made remarks: “you have zero privacy”, “get over it”. Web sites can look at one’s Internet settings and learn a great deal of information about such person. Web sites can track what a person does and web databases can include private information about individual. E-mails can be easily read by any one other that the e-mail account owner. Information about one’s interests and personal life can be gathered from public discussion areas. Someone can steal another’s password or even “steal” another’s identity. Marketing groups and companies can compile comprehensive files about an individual’s buying and Web surfing habits. In fact, people have been fired based on private e-mail they’ve sent at work. Those are just among the straight forward examples as how individual’s privacy is being compromised over the Internet. This paper persuades that there is legal solution to deter and/or remedy such privacy intrusion while at the same time formulates the acceptable concept of privacy. At the later part, this paper identifies how the existing legal principles fail to protect some aspects that warrant legal protection and how the propose concept of privacy will cater to that need.

2. Privacy

What is privacy? The proposal here is that what people refer to as privacy is actually individual’s freedom of private life. Being a person who lives, an individual has the right to live his life the way he wants it to be. As part of that, one has the right to decide what to do or omit about his life. Since an individual does not live alone, his wishes and desires subject to that of others, of the society or community around him. In other words, one’s “right to live his life” is subject to that of others.
Therefore, the scope has become narrower and the freedom that individual should have is restricted to such freedom within which context the exercise of his freedom does not infringe or interfere with that of others. That can be assured in situation safeguarded with two touchstones. First that the activities one intends to do is private. Second, the exercise of such private activities is done within a private sphere. That necessitates further elaboration of what is or will be considered as private activities and which situation is or will be considered as to fall within private sphere.

### 2.1 Private Activities

The issue whether or not certain kind of activities is private is a very objective one. There may be situation where one thinks that what he does is private while other somehow believes that it is of the latter’s interest too. Similarly, there will be situation where one believes that he should be “let alone” yet others would not allow him so for the former’s own good, at least to the opinion of the latter.\[\text{2}\]

It shall be noted that ‘an activity is not private simply because it is not done in public. In does not suffice to make an act private that, because it occurs on private property, it has such measure of protection from the public gaze as the characteristics of the property, the nature of the activity, the locality, and the disposition of the property owner combine to afford.’\[\text{3}\]

It is submitted however, that so long what one intends to do is or will merely be directed at or affecting his own body or soul, such activities would be considered private. Private activities include anything that an individual can do or omit to do to himself, including but not limited to what one can do or omit about his physical identity, physical and psychological integrity,\[\text{4}\] and the authority over his body. What one eats or drinks or applies to his body or wears would be his private matter that no other should dictate him to do otherwise. Even the decision whether to eat or drink or wear something or wear nothing is also private. Based on the same principle, one’s choice of what to believe (eg, one’s thought about religion or faith, the choice to be an atheist or even the choice not to choose or exercise any thought whatsoever about a faith or religion), how he’d like to do about his sexual life (sexual orientation, fantasies, etc), whether to participate politically or otherwise would also be private matters – as long as he keeps all those to himself. In short, private activities vary and include anything that one wants to do or omits to do provided he does it only to himself without involving any other person.

On the basis that only the activities that directed to a person himself can be called as private, all criminal intents or torts will not be protected regardless whether the preparation for such has been done in private for such action is directed towards other/s. No action that is solely directed to a person will give rise to criminal liability. If one intends to end other’s life, his intention is criminal and he cannot hide behind the shield of privacy or allege that such action is his private matter – as that can only be achieved by affecting the same on other/s – thus does not fall within the ambit of private activities. No crime, however, will be committed by a person who addressed the act of killing unto himself (suicide). Similarly, torture is a punishable crime if the same is to be effected on others, but not when the same act is being performed merely unto the person’s body. Thus, for example, tattooing or body piercing will amount to criminal offence when affected on non-consenting individual but not otherwise. Similarly, creating noises may create nuisance but it is not if such person ensures that the effect of such noise is directed merely to himself, eg, by sound proofing the place where he will make the noises. Put it the other way round, no person will successfully pledge protection on the ground of privacy for commission of a crime – putting aside the legality and illegality argument – for it will surely fall beyond the first touchstone of the privacy. Maximum seclusion of one person does not warrant him the right to privacy – regardless the extent of seclusion he may secure while doing the action, if such action is not merely directed or meant to be effected solely upon himself.

The scope of private activities may also be broader that is when other person involves in what otherwise would be a private matter. Such involvement of other or few others will not alter the privacy nature of the activity provided, in addition to the basic principle that mutual consent is the
basis for the involvement, the parties must have common understanding about the privacy of such activity.[5] Thus when the parties involved have the common understanding about the privacy of the activity, body piercing, tattooing, cosmetic surgeries, transsexual surgery or even sexual intercourse are considered private while the same may not be achieved or effected without the assistance or participation of other. Those are among the examples where involvement of others does not negate the “private” nature of activities. Whether there is any legal implication or as a result of what otherwise is a “private” activities is not within the context of this paper.[6] Similarly moral value, whether or not what one considers private is acceptable to the moral value generally observed in a society where such person lives, is not the subject that will be discussed in this paper.

It is suffice to say that so long what one intends to do is directed to himself should be considered as private activities, with or without the participation or assistance of consented other with understanding about the privacy of such activity, until the same has been negated by the absence of the other touchstone, ie, its exercise within private sphere.

2.2 Private Sphere

What is private sphere? As the term itself implicate – private sphere simply means the circumstances within which one can reasonably expect to have privacy.[7] There is no straightforward formula for that. One cannot simply name a place and consider such a place will guarantee his privacy without further elaborating the “condition” of such place. It is very subjective and must be seen on case-by-case situation. For instance, while one can easily feel that he should have privacy while being in his bedroom in his own house, his claim for breach of privacy may not success against a person who unintentionally saw him nude through the window of the former’s bedroom while the curtains are wide open. Neither the claim should stand, even if an activity that otherwise private is carried in a ‘closed’ area, if such activity is being carried in the presence of too many people that a reasonable person cannot expect privacy.[8] Thus the European Court of Human Rights in Laskey, Jaggard and Brown v. United Kingdom[9] noted that:

“…while there can be no doubt that sexual orientation and activity concern an intimate aspect of private life, however, where a considerable number of people were involved in the activities in question ..., it may thus be open to question whether the sexual activities of the applicants fell entirely within the notion of "private life" in the particular circumstances of the case.”[10]

On the other hand, while a restaurant is not usually considered as private area, a claim for privacy infringement should succeed if the claimant has specifically requested for his privacy; the place where he is going to dine was supposed to be out of the sight and hearing of others and that he has been given assurance about his privacy by the restaurant staff – yet, without his knowledge, the restaurant has installed hidden camera that monitored and recorded his every movement. Thus, base on the particular circumstances of each case, the expectation of privacy was upheld in public premises that are being rented for exclusive private function, hotel rooms,[11] hotel swimming pool[12] and even a ‘private island’[13]

Concisely the second touchstone can be interpreted as that a privacy claim will not stand if the place is of such condition that it is not reasonable to expect for privacy[14] but the same will be upheld, even in public premises if the expectation of privacy is reasonable based on the particular circumstances of each case.

Applying this touchstone in the light of the first touchstone, take for example public nudity. Most countries would consider public nudity is unacceptable to protect the moral of the public and the prohibition against public nudity is rested on the ground of public interest. Let set aside the public interest issue, would one be allowed to argue that the freedom of private life will afford him the right to be nude in public? While it is completely accurate to say that the choice about what to wear or not to wear anything is a private decision and thus falls as within the scope of private activities, the right to privacy will not be afforded for the private activity here has not been exercised within the private sphere. Outside the private sphere an individual’s life, desires and wishes are subject to the
reciprocal rights of others and those of the public. While he has the right not to wear anything, the public’s interest demands that the public shall not be subjected to a situation that may cause an embarrassment or being “forced to face” what they don’t feel comfortable to, not at least openly or publicly. Another example is when personal secrets being blatantly communicated in a public. For this point the submission shall be read first in three (3) conjunctive tiers – they are:

1. Privacy is the concept that includes the autonomy right of individuals upon his private life;
2. The autonomy empowers the individual to determine what he likes to do about his private life – including for instance the right to disclose personal secrets;
3. The extent of autonomy includes the individual’s right to dictate what the recipient of personal secrets may do about the information.

All these three are falling within the ambit of the first touchstone of the privacy and thus they are to be read with the second touchstone – which resulting in that the claim for privacy is only valid where the same is exercise in the manner where one can have reasonable expectation of privacy. In the given scenario, one’s privacy does not cease to exist when the personal information has been communicated in private. Consequently, there is a breach of privacy when the personal secrets that was communicated in private is subsequently being published or used in any manner without the consent of the owner of such secret – regardless the value of such information and whether or not the information may be afforded protection under the law of confidence (eg, if the information is available in public domain). On the basis of the same analogy, while one’s privacy includes his right to make public what otherwise is private secret, he will not be allowed to claim the right to dictate others about what to do with the personal secret (the third tier) if the same has been blatantly communicated in a public – for until then the second touchstone for privacy ceases to exist. (Not to say the freedom of expression that the public has)

It shall be noted that the amplitude of private sphere is not merely determined by location or whereabouts of an individual. Private sphere can also be established depending the way how an individual preserve private facts. For example, regardless of an individual’s locality, private sphere is established for those parts of his body that he tried to cover, that he does not want the public to look at. Thus, one claim’s for privacy will not stand if others stare or look at the “open part” of his body while being in public. It may be rude to stare at a woman’s chest but that alone does not amount to invasion of privacy if such a woman, while attending a public function, has herself divulged that part of her body by wearing a cloth revealing part of her chest. Neither is there invasion of privacy if a member of public makes a record about the revelation of part of that woman’s chest or even takes her picture. That part of her body is not “kept” within private sphere. If a person from the next building uses additional device, eg telescope, and looks at that woman’s chest, the fact will remain unchanged, that is privacy will not deter such ‘observer’ from doing so for as long as the “disclosure” is made publicly. The mere fact that additional device has been deployed will not enable any claim for privacy while the same is not applicable against other observers who do not deploy any special equipment. On the other hand, if one has taken necessary precaution to cover any part of the bodies to exclude public observation to that, the use of an x-ray device to allow a person to look at the covered part of the body, regardless of such individual whereabouts, amount to intrusion of privacy because the fact that one takes precaution by covering the parts of his body establishes the private sphere for that parts of her body. Similarly, there is invasion of privacy if a picture has been taken by a special x-ray camera that allows the prints to reveal what cannot be seen by ordinary eyes. That principle shall be applicable for a person who covers any part of the body for any reasons, for examples, such parts had been badly disfigured in fire or religious belief, or for a celebrity who wears disguises to evade public recognition.

With the two touchstones in mind, one’s privacy really is his freedom of private life. If legal recognition is being afforded to this concept, one’s privacy can be legally secured both in real life and in the digital world.

3. Technology and Privacy
Decades ago, it would be much easier to ensure that one is within a private sphere simply by ‘placing’ oneself within an area where no other is there and such area had sufficient measures of protection from public gaze. One, thus, could feel secure about his privacy while being within his premise, in the hall of his house, bathroom, kitchen, room, etc – provided the windows and curtains are closed. Presently similar state is more difficult to achieve due to the advance of surveillance technology which will allow the observation to be effected penetrating walls, etc. seclusion of oneself, is not sufficient in the context of digital world. Not only that is almost impossible in practice but also the same will not guarantee that one is not subjected to surveillance even in the place or manner which – as far as he knows – should afford to him seclusion from others.

The advance of technology creates threat to one’s freedom of private life in so many ways not imaginable before. In his novel ‘1984’ Orwell narrated that:
"The telescreen received and transmitted simultaneously. Any sound that Winston made, above the level of a very low whisper, would be picked up by it; moreover, so long as he remained within the field of vision which the metal plaque commanded, he could be seen as well as heard. There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time. But at any rate they could plug in your wire whenever they wanted to. You had to live - did live, from habit that became instinct - in the assumption that every sound you made was overheard, and except in darkness, every movement scrutinised."

Today CCTV cameras use infrared technology and can see in the dark and can zoom in beyond normal human visual range, and no longer need a wired infrastructure, but can work over mobile phone networks or wireless LAN. The video and audio signals can be processed electronically to automatically attempt to pick out an individual’s face from a database of suspects using face recognition software. There is even research ongoing into classifying "suspicious" behaviour automatically from video images. Such CCTV systems have already been linked to automatically fire military weapons systems. Further the use of any x-ray equipment will allow his movement to be watched. In fact, regardless of whether or not any light is present, the ultra-sound like of equipment can still record every single movement made.

In the new digital world, the internet poses the situation never imaginable before. While one’s every movement can be watched, recorded and accordingly interpreted by means of CCTV cameras, use of royalty cards, credit cards, debit cards, makes tracking of one’s habits become easier. The introduction of electronic databases linked with the databases available on the internet and the databases linked with the citizens’ national ID cards or social security cards or drivers’ licences enables surveillance and allow that to be done effortlessly. Internet, does contribute towards the same effect. Thus, before the legal attempts to secure privacy will be examined, the paper will briefly show how the technology can be employed both to invade and protect privacy. While technology surveillance can take place in both real space and cyber space, this discussion in this paper is limited to such in the cyberspace.

### 3.1 Technology v. Privacy

Nothing in the world is offered for free. Everything provided or given to another party must be based on some acceptable returns, if not in term of cash or economic gain in one way or another either directly or indirectly; it may also be given or provided for love or affection. Most of the what we though as “free” facilities being offered on the internet is really being offered on some other expense, it may not be money but there must be something else. Usually, the understanding is that the user of such facility “must agree” to dispense with his privacy to some extent – upon which the facilities provider may generate income from others or in other manners. For example, some “free” web-based email providers offers 1 gigabytes of email storage (Gmail, Walla, Gawab), but before starting using such service, one must carefully read the terms and conditions of the respective service.
provider, especially the one printed in fine print. Eg Gmail reserves to right to scan every email and also provides adverts on its email service. Thus, when a facility is said to be provided for free, those who value and have concern about privacy must ask – at what expense such facility may be offered for “free” and whether that will be acceptable as against the value that one has to pay for it, eg, compromise of one’s privacy.

Instant Messaging (IM) services such as Yahoo! Messenger, MS Messenger, AOL, ICQ, etc. allow its users to communicate with the listed friends almost instantly. The users will appreciate the service as something that facilitate easy and fast communication, sometimes without even realizing that whatever he types or says over such facilities can be scanned and read or heard by the services providers.

Tracking cookies are an invaluable tool for marketers/advertisers as users online experience can be somewhat targeted. Demographic data collected from these can be used in a multitude of ways as how real surveys are used. Websites place cookies to monitor the visitors’ behaviour – the way CCTV cameras do to anyone who passes the area within its range – but in a more comprehensive, wider effect and more lasting manner. The cookies can do much more things that even CCTV cameras cannot do. The surveillance and data being collected through the use of cookies go beyond the boundaries of such website. The data can still be collected even after the visitor has left the website. Most of cookies meant to facilitate the visitor, such as to allow the visitor to spend less effort and time the next time it returns to the same site but the cookies are also used to allow the services or facilities providers to track the visitor online behaviour so that it can target and select the ads that it feels is of the visitor’s interest, based on the visitor’s activities pattern, either by sending the ads to the visitor’s e-mail or displaying the same when the visitor returns to the site. In addition to collecting demographic data, a surfer’s behaviour is also recorded and its habit can be interpreted on the basis of the type of the sites it visits or browses, including, for instance, the links that such surfer has clicked (Clickthroughs). While any of the above are not intended and may not be used for malicious purposes, the data being gathered may be used by anyone to achieve the result unwarranted by others.

In more extreme way, the Adware, Spyware, Trojan Horse and Backdoor may be employed in order to gather data and Internet usage or online behaviour. Valuable demographic data are being sold to advertisers and in return, targeted ads are being effected. Some important data of users such as credit card numbers, social security/national insurance numbers, bank accounts (including username and passwords), etc are also being collected. To some extreme level, the Trojan Horse, for instance, allows one to control another users’ pcs without the knowledge of such users. The one that gains control over the other user’s pc then will be able to use such pc for malicious activities, eg, using the pc or spamming purposes, to open proxy (either amounting to hacking or cracking), Denial-Of-Service (DOS) attacks for commercial or personal gains. In any cases, such users are just like zombies, while the control of its pc lies in the hand of another. Regardless of the actual location of internet user, any of the above may occur – whether or not the pc is used for personal purpose from home, official purpose from workplace or both.

The recent trend of privacy intrusion over the internet will includes snoops, either by individual, commercial bodies or even a government. Today technology offers such facilities at a very affordable cost. As a result, instead of asking why any one snoops the question has changed into – why not? The cost for snoops per gigabytes (not megabytes anymore) has gone down very considerably for the past few years. Even desktop versions of 250 GB harddisk are available to mass public. Introduction of SATA (Serial Advanced Technology Attachment) provides cheaper and viable alternative to SCSI (Small Computers Systems Interface), as normally found in servers. Cheaper servers which storage uses SATA are now available not only faster but also at much cheaper cost. Thus, the idea becomes ‘why not snoop/copy/log everything if the cost for such has ceased to be a determinant factor.

Bandwidth also is another why not factor in this case. With the introduction of cable/ADSL
(Asynchronous Digital Subscriber Line)/broadband, users are now connected longer and with a much larger bandwidth. As broadband becomes cheaper, more and more users are online longer and some do have their computers connected 24 hours a day, seven days a week. Hence the prevalence of spyware/adware/Trojan horses/backdoor, which can make use of these computers. The longer a computer is connected to the Internet, the more susceptible is it to hacks/cracks etc.

3.2 Technology for Privacy

Despite offering those facilities that may compromise individual’s privacy, the technology also offers facilities that can be employed in order to secure one’s privacy. The first shield that one may want to consider placing for the protection of his privacy is by using firewall. The firewall will act as the first line protection for its user and a shield against hacker or cracker. A good firewall will monitor both incoming and outgoing traffic. A computer has about 65000 ports that can be used to share information with the Internet or other computers. It is best to set the firewall to deny all access first, then enable one by one as may be required. The user can set the firewall to alert him on all access.[19]

In addition to that, every computer user must use anti virus software. It has become necessary that every e-mail sent and received from the Internet must be scanned as Adware, Spyware and viruses that may compromise the user’s privacy may come through an e-mail and since the variation of virus changes, it is important that the user regularly update the antivirus software.[20] Internet user needs also to use Spyware/Adware removal software. Such software should be used before shutting down pcs after the user was online AND after restarting pc, every single day. Sometime the user needs to use a combination of software as some adware/spyware are very elusive.[21]

Be anonymous as far as possible.[22] Use free and anonymous email accounts such as Hushmail, which provides anonymous and encrypted email accounts;[23] DodgeIt email provides free open email accounts so anyone can use while registering or when providing information on the Internet. Emails from the account can be checked without passwords. Thus, if one needs to give email address but is concern about giving his e-mail address, such person can use Dodget.[24] It is also helps to use passphrases instead of password. Passphrases can be a long phrase from the title of one’s favourite song, words of wisdom etc, keeping or inserting a few non conformance letters/characters along the way (eg. YellowSubmarine/YellowSubmarine or IHateMySelfforLovinYou!) The advantage of using passphrases is that Passphrases are much easier to remember than PINs/passwords. It will also be very beneficial if one does not leave his email address lying around on the internet and make a habit of using “name at domain dot com” or name@dontspamme.domain.com instead of giving/writing one’s real email addresses (name@domain.com) online. This will deter email harvesters (software which goes around the Internet searching for email addresses, a spammer’s tool) for using such e-mail address and that, to some extent, works as protection against spammers.

It is a good practise for one to do once in while a search for his name, ID number (if applicable) or any other info related to himself and see what comes up in search engines. One might be surprised on what he finds out. When such individual finds something personal or simply unwarranted being written somewhere, such person shall contact the party with haste and request to have it removed. Apart to that, one should make the habit of clearing cache after using online banking services especially when using public computers. When surfing to encrypted sites or secured websites (SSL-Secure Socket Layer), make sure the padlock icon is on and not broken or unavailable. Do click on the padlock to make sure that the secured site being visited is actually what it is and not otherwise. Although it is just a simple thing to do, it is necessary to always lock a pc when leaving it unattended even for a short period of time. A spyware/adware/Trojan horse/backdoor/keylogger software takes only seconds to install. In addition to all those, one must be extra cautious when using any Peer-to-Peer(P2P) software such as KazaA, Grokster, BearShare etc. as these are most of the time are full of malwares.
When one is using the Instant Messaging service, one can use additional services to allow the communication to be carried in a secure manner. To mention a few, Secway secure YM/MS Messenger/ICQ add-on — Uses public key exchange (www.secway.com); Trillian (free multi protocol (YM/MS Messenger/ICQ/Trillian) chat client) secure messaging — Uses 128-bit randomly generated session keys (http://www.ceruleanstudios.com); ZoneLabs:IMSecure(www.zonelabs.com). They can be either the free versions with limited functionalities and only for non-commercial use or paid versions that have more functionalities.

The use of wireless LAN security may also open the door for privacy intrusion. Unsecured wireless LAN network allows intruders to snoop/listen and capture network activities. In order to secure the wireless LAN network, one needs to enable WEP (Wireless Equivalent Privacy). Almost all Wireless-Fidelity (WiFi) certified products are capable of this. Even though it may not be as secure as more recent (WPA) but at least it does provide a layer of protection and the best of all that is free. Then, the user shall change the default manufacturer’s SSID (Service Set Identifier) to anything which should not be related in any manner to him. In addition to that, he needs to disable “broadcast SSID” as the default setting of this is enabled. With broadcast SSID disabled, an intruder is playing a guessing game on getting the SSID correct. The SSID on the intruder’s machine must match that of the SSID of the network, otherwise he will not be able to access your wireless network while if SSID is set to broadcast, the access point will accept any SSID. For more advanced users, one can try disabling DHCP (Dynamic Host Configuration Protocol) and set IP’s of each of the network client manually. The other thing one could do is to set MAC (Media Access Control) address access control and only allow those clients with their MAC addresses registered in the access point to have access to network.

3.3 Technology and Legal Protection of Privacy

While many attempts taken to afford more protection for individuals while online both from legal and technological ways, the attempt is still proved to be futile. As Scott McNealy of Sun Microsystem declared: “you have zero privacy anyway” That statement is accurate in the sense of one’s condition while being over the net. But we don’t have to “get over it” as suggested by Scott McNealy as there is still a way to afford the privacy upon people on the net. Legal protection is one of the methods being employed to address any issues for which any other factors may not provide remedies. In the context of legal protection, privacy is usually associated with two major factors, ie, secrecy and personal data protection. This paper seeks to prove that a mere judiciary recognition for the concept of privacy as in this paper will afford sufficient protection to privacy even in situation where both the data protection principle and law of confidence will fail to do so.

Among the contention brought against the idea of having legislation protecting the right to privacy is that, the law of confidential information provides sufficient protection for the aspect of privacy. To rapidly dismiss this claim, it is appropriate to quote what Lord Nicholls of Birkenhead rightly noted in *Campbell* that “an individual privacy can be invaded in ways not involving publication of information. Strip-searches are an example.”[25] And thus it becomes obvious that privacy is not solely about protection of information.

As suggested earlier, the idea of privacy is to ensure individual’s freedom upon his private life and not merely to protect some aspects of it and allow others to intrude upon the rest. Many people have common misconception about privacy.[26] That, perhaps owe to the influential definition offered by Westin that “privacy is the claim of individuals, groups of institution to determine for themselves when, how, and to what extent information about them is communicated to others.”[27] Consequently when one talks about privacy, one will easily associate the context of speech within the scope of secrecy. Thus, it is not surprising that one will equalise any legislation that protects data as privacy legislation. It is submitted that the notion for privacy shall encompass wider scope of individuals’ interest and should not be restricted merely to one’s exclusive control over his personal information. At this point, it is worth to cite what Kent Greenawalt once emphasised about the scope of privacy, while rejecting the limited definition given by Westin.
“There are some situations where disclosure of information is involved in a loss of privacy but it is not the only element, or even the primary element, in the invasion of privacy… A person who is raped or brainwashed has suffered an extreme loss of privacy, and any information the intruder may have obtained is quite incidental to the major harm. An unwanted police search of one’s home is disturbing to familial privacy entirely apart from whatever information the police discover. Thus loss of control over information may often occur as a consequence of an intrusion that is independently disturbing to one’s sense of privacy.

Another whole aspect of privacy which the Westin definition does not touch is the freedom to make choices about one’s behaviour in respect to private matters. … The ‘privacy’ that is primarily involved in these cases is not freedom from unwanted disclosure of information of freedom from actual intrusion into a private situation, but freedom to live as one wishes in respect to certain private activities.”[28]

To equalize the scope of ‘privacy’ with the common law of confidence is a misconception that needs to be rectified. If information has been communicated to a person on understanding that such person shall not disclose it to another, there is a breach of confidence upon disclosure, regardless if the information is personal or otherwise, however it will only amount to violation of privacy if the information so disclosed is personal. Individuals would definitely regard confidential information about his private life as part of his privacy, nevertheless, not all confidential information is necessarily about an individual’s private life – thus part of his privacy. For example, it is very well established that trade secrets are protected as part of the common law of confidence,[29] yet these data unmistakably are not part of individual’s ‘private’ life. Similarly, some corporate information, some of which do not form as part of trade secrets, may be qualified as confidential information. However, so long such confidential information does not relate specifically to an individual, such information shall not form part of informational privacy. Conversation during a meeting and reasons in deciding the award of some projects, funding or scholarships may be confidential yet those communication will not legitimately form part of privacy. Conversely, some matters are considered private, though it may not be a confidential information, for example, individual’s personal data such as a person’s name, address, phone number are not confidential, at least, not to the people who habitually deal with such individual, and because such information are readily obtainable by consulting the local telephone directory, and nowadays, from the Internet. Similarly the information about matrimonial proceedings in court involving an adult or those of an individual’s direct relatives such as parents or siblings are will not be considered as confidential as these information are readily available by consulting the court records or legal reports, yet one may be allowed to argue that such information is private and thus, for example, a person may legitimately be granted an injunction preventing other to tell the whole neighbourhood that the former, the new comer in the neighbourhood, has got his parents divorce because of his father adultery. [30] The recent injunction granted to Maxinne Carr, that includes prohibiting journalist to publish about some of her new personal data, aside to the fact that the injunction is meant for her safety, the end result of such injunction is an example that while some personal data may not be confidential in the sense that such data may be easily collectable by one means or another, its publication may be restricted.

Aside to the fact that not every aspect of private life involves data and even those private data are not necessarily confidential, to apply the elements required for the common law of confidence as established by the Court of Appeal in Saltman Engineering Co. Ltd. v. Campbell Engineering Co. Ltd.[31] and were summarised by Megarry J., in Coco v. A. N. Clark (Engineers) Ltd.[32] will not be appropriate for the notion of privacy. It is well established that for a breach of confidence to succeed the three elements must be satisfied, namely that the information itself must have the necessary quality of confidence about it; that information must have been imparted in circumstances importing an obligation of confidence; and there must be an unauthorised use of that information to the detriment of the party communicating it.[33] To impose the fulfilment of the elements for breach of confidence cases to breach of privacy cases is not desirable.

The first element requires the information is to be confidential. That may include technical, commercial or personal secrets. While personal secrets will entirely be part of privacy, technical and
commercial secrets will not. Conversely, personal secrets are always private matters until long the owner of such secret reveals them to the public, however under the law of confidence, confidential secrets will not be considered “confidential” anymore once such information becomes available in the public domain, regardless the manner how and by whom the information being disseminated.[34]

The second element, that the information must be imparted in confidence, requires the confidentiality in the manner of communication and restricts the duty of confidence to the person to whom the information is imparted, but not to a stranger or a third party. The basis of equitable intervention to protect confidentiality is that it is unconscionable for a person who has received information on the basis that it is confidential subsequently to reveal that information. Although the relationship between the parties is often important in cases where it is said there is an implied as opposed to express obligation of confidence, the relationship between the parties is not the determining factor. It is the acceptance of the information on the basis that it will be kept secret that affects the conscience of the recipient of the information.[35] In other word, the jurisdiction is based not so much on property or on contract as on the duty to be of good faith,[36] as Bingham L.J. in the Spycatcher case, said, at p. 904: "The cases show that the duty of confidence does not depend on any contract, express or implied, between the parties. If it did, it would follow on ordinary principles that strangers to the contract would not be bound. But the duty 'depends on the broad principle of equity that he who has received information in confidence shall not take unfair advantage of it."

The above, nevertheless limit the duty of confidence to those people to whom the information has been communicated. Such duty is not extended to a complete stranger who overhears secret conversation or to whom the information is mistakenly or unintentionally disclosed. Either way, it is arguable that the circumstances do not import an obligation of confidence, and thus, the duty of confidence does not arise.[37]

The classical cases of breach of confidence mainly deal with the situation where the recipient of an idea had benefited from the commercial use of such idea by excluding any profit to the actual owner of the idea[38] or simply an attempt of disclosure in disregard of the duty of confidentiality.[39] In some cases the protections being seek for information that was private in nature and sometime the confidential information is not of private nature. However, the fulfilment of the third element may difficult to achieve where the publication or use of the information does not benefit the recipient neither it causes anything to the owner of the information but personal embarrassment. In Stephens[40] even though Sir Nicolas Browne-Wilkinson V.C. expressly excluded himself from examining the third element for breach of confidence,[41] the disclosure, followed by publication, of the information relating to sexual conduct of a lesbian nature between the plaintiff and another to the press would presumably allow both the recipient of the information and the press to earn monetary gain. As submitted earlier, privacy as cause of action will stand regardless the presence of loss or damages to the plaintiff. Consequently it will not be affected with the absence or presence of benefit to the defendant while that may affect the quantum of damages to be awarded to the plaintiff.

Finally and most importantly, privacy is not only about secrecy. The right to privacy, as an individual freedom to do or omit to do about his private, will include one’s decision to publish some of his private facts.[42] It is submitted that when one opts to reveal some personal information to public, he does so in the exercise of privacy and thus, while the publication of public facts makes such facts no longer ‘private’, such publication is an exercise of one’s privacy right. Consequently, if a legislation were to be introduced to prohibit individuals from disclosing some kind of private facts, such law – unless rightfully justified - would amount to intrusion of privacy, in the sense that it would limit individuals’ freedom of choice whether or not to disseminate or publish about his private facts. However, such legislation would not in any way be contrary to the principle of law of confidence and would definitely preserve secrecy.

In addition to all the points discussed above, in the context of cyberspace each of the elements for the cause of action of breach of confidence may turn to be a hindrance. The requirement that the
information must be confidential, will itself give approval to many unwarranted privacy intrusion solely on the basis that such activities are not based on usage of any confidential information. It is a widely acceptable norm that one should not expect secrecy while conducting online activities (except, perhaps when on secured sites or when any communication is encrypted). However, most of activities which should amount to privacy intrusion are based on mere use of non confidential information, such as demographic data, or as little as e-mail address. Spammers use that information in sending spam, sometimes coupled with the online habit of the addressee and most of the times, in disregard of that. The advance of technology (brute password attack) will allow the privacy intruder to secure access to another’s e-mail account, scans/searches for any e-mails, or simply reads all the e-mails in such e-mail account. All that the intruder needs to obtain in order to target a person and subjected the latter to that is the latter’s e-mail address and that is unlikely to be considered as confidential information.

The second requirement is that the information must have been “communicated” in the circumstances imparting the duty of confidentiality. While this part of obligation has been relaxed in the sense that pre-existing confidential relationship between the parties is no longer required,[43] the nature of the Internet makes even the relaxed rule is difficult to meet. The prevailing view is that, any Internet communications or activities being held in “open” space is similar to those activities that one does openly in public in the real space. One’s argument on confidentiality about what he writes on a postcard will fail as much as those communications exchanged over the Internet, either through e-mails or by way of instant messaging services. The same applicable to any information submitted in non-secured web sites. While the argument may be substantiated if the originator of such communication takes extra precaution by encrypting his communication or using secure access to any web-sites, collection of data or gathering of internet habits from other online sources such as search engine and most of unsecured web-site will suffice to allow intrusion of privacy. Can a person object to intrusion of privacy based on the cause of action for breach of confidence if such intrusion is based on the observations of his online activities? Hypothetically, if one publishes a general statement that “A” a prominent religious leader has visited several “adult” websites and substantiating that allegation with several occasions where such websites have been visited, in some occasions the sites were visited by way of clicking some links to the internet addresses as provided by a search engine – would not that amount to privacy intrusion? The case for breach of confidence will obviously fail as not information has been communicated in circumstances imparting the obligation of confidence. Would not the absence of suitable legal provision to deter such publication cause unnecessary stress or even depression to “A” and those others who might be directly related to him and impacted by any damage to his reputation. What if what A has done was nothing more than clicking the links he obtained from the search engine under genuine belief that he was visiting something else (some “adults” websites may use a very general and sometimes misleading keywords). What if he has done nothing but to research on some matters for his background knowledge in the matter? Above all those, what he has done nothing but his private matter, why would not the law provide any remedy for the damage he suffers?

The third element for the law of confidence is as difficult to prove as the first two. Intrusion of online privacy may occur in the situation where no data had been used at all by the intruder. For example when the intruder simply scans and reads e-mails for his pleasure or when data are merely being collected without ever being distributed. Even in the most extreme situation, no unauthorised use of information may have involved, for instance, when Trojan horse is used to control the other’s computer. Does not the absence of legal protection for that is equivalent to allowing a person to install CCTV cameras in the house of another without the latter’s knowledge and consent, obtaining the access to view and record every movement in that house? Would not that obvious example of privacy invasion and yet the same is not protected under the law of confidential information for the absence of unauthorised use of such information. One may argue that so long the information is not being published, no damage is done to the victim of such intrusion, then the very simple question one should ask is, what if the same happens to himself? Would he like or allow himself to be subjected to such observation? Would not he want freedom upon his private life?
That illustrates that privacy is not only about secrecy or protection of confidential information and it is apparent that the common law principle of law of confidence fails to afford protection to individual’s online privacy in most circumstances.

It is also submitted that privacy is not merely about protection of personal data. Thomson argues that “if we use an X-ray device to look at a man in order to get personal information about him, then we violate his right to privacy. Indeed we violate his right to privacy whether the information we want is personal or impersonal. We might be spying on him in order to find out what he does all alone in his kitchen at midnight; or we might be spying on him in order to find out how to make puff pastry, which we already know he does in the kitchen all alone at midnight; either way his right to privacy is violated.”[44] As illustrated earlier, invasion of online privacy may occur not based on the use or act of processing of personal data. It is very easy to deduce a fact – which sometimes may be really private – by using the internet and sometimes without the need to employ the personal data of an individual. Cookies stored on a person’s computer will allow a web site to recognise such entity the next time he/she visits that website. That alone will allow one to easily infer what kind of matters that will be of interests to such person and what the persons will be looking from the Internet. For example, when one spends quite substantial time to search for information regarding the symptoms of pregnancy, pregnancy test kits and a few months later the same person searches for information related to baby supplies, the inference is such person conducting the search has become pregnant or at least the search is conducted for a person who has become pregnant. (what if supposedly the person who scan the searches know the individual personally and know that such individual is still a minor, etc, does not that will implicate further bad inferences against the search engine user?)

Similarly, if one repeatedly visits a site that supplies some sexual related items that would allow inference as to how that person’s sexual life is. On the other edge of examples, if a user which ip address indicates that he/she is located in some area known for its commitment to religion has clicked (either intentionally, accidentally or by mistake) on a link of a website which contents are such that would not be acceptable to the person professing the same religion as such visitor, that may give inference that such person is not religious enough. Regardless of any argument that may be given in relation to those examples, the above illustrate as how some very personal inferences may be deduced from non-personal data and how the same may place an individual in what may be embarrassing situation. Such matters are private and should not be of concern to others and should warrant legal protection in order to preserve the freedom of private life.

Furthermore, while it seems that the Data Protection Act 1998 is a piece of legislation that will be very useful in order to protect individual’s right to online privacy. The applicability of this legislation, however, is restricted, among others, only if the data controller is established in the UK and the data are processed ‘in the context of that establishment; or the data controller is established neither in the UK nor in any other EEA State but uses equipment in the UK for processing the data otherwise than for the purposes of transit through the UK.[45] Thus, obviously the legislation is not applicable if the data is being processed in any countries other than UK and EEA State such as Australia,[46] Far Eastern countries, etc. Beside necessitates that an individual needs to ensure that the data controller meets either of the above condition in order to be given protection under the Data Protection Act 1998, the area restriction is too limited taking into account the borderless nature of the Internet.

Since the legal attempt to afford protection is not seen to be very useful, the best advice one can give for those who wants to ensure his privacy while online is to be as anonymous as possible. Either in real life or digital world, being unanimous may not be the way one wants to live his life. While technology attempts to cater for such needs and it evolves towards providing the technology to combat the surveillance technology, the latter evolves as rapidly as well. Thus, what one really need is to have a comprehensive legal concept that not only deter others from penetrating his privacy (both in real space and cyber space) but also offers for remedy in case of intrusion and such concept must be comprehensive as not to be defeated by technology.

The submission here is very simple. The legislation is already in place. All that the judiciary needs to
do is to extend the current interpretation of the relevant legal provision to its actual and intended context to its full extent. It is unreasonable to interpret the Human Rights Act 1998, in particular Art. 8 of the ECHR merely to that within the scope of the law of confidence. The trend in the UK is to reject any notion for recognition of broad principle of privacy and rather make use of the currently recognised cause of action – breach of confidence being the frequently chosen alternative. [47] Recently, Lord Nicholls of Birkenhead in *Campbell v. MGN Limited* [2004] UKHL 22, while analyzing the cause of action for breach of confidence, reiterated at paragraph 11 that “[i]n this country, unlike the United States of America, there is no over-arching, all-embracing cause of action for 'invasion of privacy': see *Wainwright v Home Office* [2003] 3 WLR 1137. But protection of various aspects of privacy is a fast developing area of the law, here and in some other common law jurisdictions” and in the later part, at paragraph 17 his lordship concluded that: “[t]he time has come to recognise that the values enshrined in articles 8 and 10 are now part of the cause of action for breach of confidence”.

With due respect, such interpretation will not embrace the actual concept intended by virtue of individual’s freedom of private life. The interpretation should have applied conversely, that is to say, the principle of law of confidence has now become part of what is being protected by article 8 of the ECHR. The law explicates that by virtue of the Human Rights Act 1998, the provisions of ECHR become part and partial of the UK legal system. [48] It should be awarded the legal recognition it deserves to get and not to be read merely within the restricted limit of the UK legal system available prior to the application of such law.

In all the earlier mentioned hypothetical situations, the proposed concept will provide the required protection for online privacy (and privacy in real space alike). The two touchstones are straightforward, the privacy of activities and its exercise within private sphere. As discussed earlier, the first touchstone is objective. The ‘reasonable-man’ test will be applicable to determine if an activity is considered private or otherwise. At this point of time, no other factors, or matters will be taken into consideration. Once such reasonable person will rule that the activity in question is considered private then only the second touchstone is to be given its subjective evaluation. Either in real space or cyber space, the applicable test for this second touchstone is that “whether, taking into account all the surrounding circumstances, there is a reasonable expectation of privacy”. In real space, that can be ensured by placing one self in an area free from public gaze. Whether or not such an area is in reality is penetrable by surveillance technology is not counted and shall not justify any intrusion of privacy. By way of analogy, in cyber space one can take reasonable measure to ensure his privacy. That will suffice by adopting the technology that reasonably excludes public access to such communication for example by way of carrying internet activities solely on secured sites and when the sites are not secured, such communication is being encrypted. Internally, firewall can be considered as effective as the wall being used in real life. So long the measure taken is reasonable any intrusion by employing the more advanced technology for surveillance is not acceptable. Thus, it is submitted that all that is required is the willingness of the judiciary to further expand the existing principle to cater what the parliament has approved as part of the human rights as guaranteed in particular by article 8 of the ECHR – respect for the right to private life and set itself free from the limitations of the law of confidence as the needs arise. The tendency towards this can be found in the majority judgment of the House of Lords in *Campbell v. MGN Limited* [49] – though it has yet to be seen as settled law that the right to privacy is indeed the right that has to be respected as freedom of private life as per article 8(1) of ECHR.

4. Conclusion

The issue of privacy intrusion both in real and cyber space is an imminent issue that needs to be given serious attention. The dispute about the definition of privacy and its concept is an old issue that yet to be satisfactorily settled. If the concern of privacy intrusion has existed and substantiated long before the technology reaches its advance stage as today, the same should be even more prominent with the advance of the surveillance technology. It is not at all acceptable to deny one’s right to his privacy merely on the ground that the concept of privacy is too broad to be awarded protection.
Similarly, it is not justifiable either that such intrusion shall be allowed merely because the technology has advanced in a way that makes privacy intrusion can be done effortlessly. The proposal is straight forward – to give the full effect to the existing law, ie, the provision of the Human Rights Act 1998 that gives implementation of the conventional human rights – in particular article 8 of the ECHR. The hands of the judiciary are not tied – the judiciary is not restricted by any rule that it has to merely rely on the principle of law of confidence in interpreting the provision of ECHR. It is not submitted that the judiciary should extend its judicial power beyond what the parliament has not acted upon, but what is submitted is for the judiciary to give effect to the act of the Parliament, in this case the Human Rights Act 1998 which effects the provisions of ECHR. If privacy intrusion is the matter brought before the judiciary, the decision should be on two folds, ie, first consider if there is any intrusion of privacy, then second if there is acceptable justification that warrants such intrusion (eg. Art 8(2) of ECHR). To determine whether or not the right to privacy exists, the two touchstones as proposed in this paper are to be determined in sequence order. If both touchstones are satisfied, the intrusion is unwarranted and the intruder shall be deterred from doing the same or if the intrusion has happened, the claimant must be awarded the appropriate legal remedies unless and until the intruder can prove the existence of acceptable justification for such intrusion.

In a nutshell, the law is in existence; the call for its needs have been proven necessary; and the existing principle proofs to fail to provide protection in cases where privacy has been unwarrantedly intruded. All that is needed is to break free the judiciary from the traditional limitation that requires any claim of privacy must be based solely on the existing principle (mainly law of confidence). The refusal to extent the judiciary recognition for the right to privacy has been based on what Megarry V-C said:

"I am not unduly troubled by the absence of English authority: there has to be a first time for everything, and if the principles of English law, and not least analogies from the existing rules, together with the requirements of justice and common sense, pointed firmly to such a right existing, then I think the court should not be deterred from recognising the right. On the other hand, it is no function of the courts to legislate in a new field. The extension of the existing laws and principles is one thing, the creation of an altogether new right is another...anything beyond that must be left for legislation"[50]

The House of Lords judgment in Campbell may seed the light though it still yet to explicate the recognition for the right to privacy. If the initial reason for judiciary’s reluctance was for the reason given above – “that such matter must be left for legislation”, such reason should have ceased to exist by virtue of the operation of the Human Rights Act 1998. In the end, the principle of equity is crystal clear that equity will not suffer a wrong without a remedy – so, why can’t that be applied in cases where privacy has been unjustifiably intruded or breached?

[2] Re Roddy (a child) (identification: restriction on publication); Torbay BC v. News Groups Newspapers [2003] EWHC 2927, FD BFLS 3A[835]; CHM 1 [883.1], 1[227] The 16-year old child fell pregnant at the age of 12. The putative father, X, was a boy of a similar age to the child. The local authority began care proceedings in relation to the child and after the birth, her baby, Y. Y was later adopted whilst the child remained in foster care. As a result of media interest, a series of injunctions was granted to protect their identities. A few years later, on the child's application, the care order was discharged. The child then approached a national newspaper, in order to share her experiences in the care system. She was happy to be named and photographed for that purpose. Consequently, the newspaper's solicitors contacted the local authority giving notice of their client's intention to apply for a variation of the injunction. The local authority raised concerns in relation to the identification of Y. In that regards, the Court held that Article 8 embraced both the right to maintain one's privacy and, if preferred, not merely the right to waive that privacy but also the right to share what would otherwise be private with others, or with the world at large. Therefore, the right to communicate
one's story to others was protected not only by art 10, but also by art 8. It was also held that it was the court's responsibility and duty to defend the right of a child who had sufficient understanding to make an informed decision, to make his or her own choice. It was not, in such circumstances, for the parents, a court or any other public authority to make a decision on the child's behalf. In the instant case, the child was a person of an age and maturity to decide for herself.

[3] Gleeson CJ in Australian Broadcasting Corp v. Lenah Game Meats Pty Ltd (2001) 185 ALR 1 at p 13, para 42. There, Gleeson CJ identified that '[c]ertain kinds of information about a person, such as information relating to health, personal relationships, or finances, may be easy to identify as private; as may certain kinds of activity, which a reasonable person, applying a contemporary standards of morals and behaviour, would understand to be meant to be unobserved.' and that: 'The requirement that disclosure or observation of information or conduct would be highly offensive to a reasonable person or ordinary sensibilities is in many circumstances a useful practical test of what is private.'

[4] It was held in Botta v. Italy (1998) 26 EHRR 241 at para.32, that "... private life ... includes a person's physical and psychological integrity".

[5] Therefore in Theakson v. MGN Limited [2002] EMLR 22 – the argument for privacy should (and did) fail as the prostitutes involve do not consider whatever that took place in the brothel as privacy in the light of surrounding circumstances in that particular case.

[6] For example. some legal system makes it as criminal offence for a married person to have sex with anyone other than his spouse; some other legal system makes adultery merely as a ground for divorce; while for some society, the such is publicly acceptable. The same will go for the consequence of genital change, while the law has been ready to afford legal recognition for such change, when the conditions are satisfied, such change bring consequences, such as in term of pension contribution, etc. That, however, is not the ground for rejecting the idea of affording recognition to privacy, but rather indicate that the law has been based on imbalance basis and that alone should not be the hindrance for the right to privacy.

[7] Something to similar effect is explicated in the Press Complaints Commission Code of Practice whereby the note to S. 3 provides that 'private places are public or private property where there is a reasonable expectation of privacy'.

[8] Therefore while it is encouraging to know that Sedley LJ in Douglas v Hello! Ltd [2001] QB 967 at page 1001 para 126 held that "The law … can recognise privacy itself as a legal principle drawn from the fundamental value of personal autonomy." However, there would be no violation of privacy in the case since the circumstances from which the claim arose did not create the private sphere within which a reasonable person would have expected to have his privacy being respected. The proposition however, would not exclude the couple right to pursue their cause of action for breach of confidence, upon which the Court of Appeal had allowed their claim.


[10] Ibid, in para 36 at pages 56-57. However in this case the Court did not examine the point on its own because the point has not been disputed by the parties to the case.


[13] Sara Cox was awarded £50,000 in damages and the defendants were to pay that and the legal cost for having published, without her knowledge, the naked pictures of Sara Cox and her husband while sunbathing on their honeymoon. See: Guardian 7 June 2003. Available at <http://www.guardian.co.uk/uk_news/story/0,3604,972472,00.html> (last visited 9 June 2004).

[14] In Hosking v. Running [2003] 3 N.Z.L.R. 385 a well - known television presenter objected to the proposed publication of photographs taken of his two young children in a public place whilst out shopping with their mother, without her knowledge. Randerson J declined to grant a remedy to prevent disclosure of photographs of children because - inter alia - the pictures were taken in a public place. The same was among the reasons the Court of Appeal affirmed the judgment and dismissed the appeal.

[15] Adware is not necessarily Malware but is considered to go beyond the reasonable advertising that one might expect from freeware or shareware. Typically a separate program that is installed at the same time as a shareware or similar program, Adware will usually continue to generate advertising even when the user is not running the originally desired program. Malware is a collective term including the many varieties of deliberately malicious software, that is, software written for the purpose of causing inconvenience, destruction, or the breaking of security policies or provisions. (source: http://www.systemsmedic.com/malware1.htm#Adware – last visited on 18 March 2005)

[16] Spyware is a type of Malware that reports on the contents, status, or operation of the computer to a remote system or user. Generically this could be almost any type of information gathering software. More specifically, it usually refers to modules or functions in software that reports to the author, publisher, or service provider of an otherwise legitimate system. Spyware ranges from functions that report on version levels to the host system, through packages that report the presence of other software from the same manufacturer, through systems that gather information on all software installed including those from competing vendors, all the way to modules that report on the user's Web surfing. Justifications proposed for Spyware include the need to ensure versions are kept up to date in order to provide proper service, concerns about software piracy, concerns about use for illegal or unacceptable purposes, and the gathering of marketing information. Malware is generally considered to include programs such as DDoS clients (or zombies), logic
bombs, RATs, trojan horses, viruses, and worms. Malware is generally not considered to include unintentional problems in software, such as bugs, or deliberately written software that is not intended to do harm, such as pranks. (source: http://www.systemsmedic.com/malware1.htm#spyware – last visited on 18 March 2005)

[17] Trojan horse is a destructive program that masquerades as a benign application. Unlike a virus, Trojan horses do not replicate themselves but they can be just as destructive. One of the most insidious types of Trojan horse is a program that claims to rid your computer of viruses but instead introduces viruses onto your computer. (source: http://www.systemsmedic.com/malware1.htm#trojan – last visited on 18 March 2005)

[18] A backdoor is a piece of software that allows access to the computer system bypassing the normal authentication procedures. Based on how they work and spread, there are two groups of backdoors. The first group works much like a Trojan, i.e., they are manually inserted into another piece of software, executed via their host software and spread by their host software being installed. The second group works more like a worm in that they get executed as part of the boot process and are usually spread by worms carrying them as their payload. The term Ratware has arisen to describe backdoor malware that turns computers into zombies for sending spam. (source: http://encyclopedia.laborlawtalk.com/Malware - last visited 18 March 2005)

[19] ZoneAlarm(www.zonelabs.com) provides free firewall but a stripped down version of their Pro and Plus versions. The free version, however, is more than adequate for personal and non-commercial use.

[20] Some example of free antivirus software include: AVG Free Edition offers basic virus scanning and protection. It is however are provided for free only for its use for personal purposes. For enterprise users, AVG offers a Pro version with a lot more functions and capabilities. Another example will be AVPE:Anti Virus Personal Edition-www.free-av.com by H+BEDV Datentechnik GMBH. Again it is offered for free for personal, non-commercial use only.

[21] Among the example of Adware/Spyware removal software includes: Lavasoft’s(www.lawasoft.com) Ad-Aware SE Personal Edition - adware removal software and free for personal use. Also offers Pro version with enhanced functions. Spybot’s(‘direct download from CastleCops http://computercops.biz/downloads-file-108.html)Search & Destroy-removes spyware v.3.2 – Free software for personal use JavaCool’s(‘www.javacoolsoftware.com/sbdownload.html)SpywareBlaster v2.2 – stops spyware from... installing in the first place. JavaCool’s(www.javacoolsoftware.com/spywareguard.html)SpywareGuard v2.2 – protects from spyware in realtime. Both software from JavaCool are free and donationware. Codestuff Starter(not really a spyware remover but essential as to keep track on what's being run at boot time and also provides detail on running applications in pc, even hidden ones)

[22] Free anonymous proxies are available online. List is here http://www.atomintersoft.com/products/alive-proxy/proxy-list/ Eg, anonymiser.com, proxydom.com, guarster.com, Even better SSL based proxies(normally paid service) are also available.

[23] www.hushmail.com, free accounts are limited by the functions available to paid services.

[24] www.dodgeit.com The service is provided for free. However, if one likes to have a control over a particular dodgeit address, one can make donation and such person will be granted exclusive access to such account.


[26] For examples Phillipson, G., ‘Transforming Breach of Confidence? Towards a Common Law Right of Privacy under the Human Rights Act’, [2003] 66 MLR 726 at page 732 defines privacy as ‘the individual interest in controlling the flow of personal information about herself’; Parent, W., “A New Definition of Privacy for the Law”, Law and Philosophy, 2 (1983) 305 at page 306 proposed privacy to be defined as “the condition of not having undocumented personal information about oneself known by others.”. Even the article written by Warren and Brandeis emphasised on the privacy as the right to control the publicity against embarrassing ‘private’ facts. That, however, should be interpreted in the light of the incident that triggered the writing of such article, and not meant to limit the scope of privacy merely to such aspects.


[29] See for example Faccenda Chicken Ltd v. Fowler[1985] 1 All ER 724.

[30] In the same manner with the given hypothetical situation, In re S [2003] 3 WLR 1425 the Court of Appeal had to strike the balance; on the one hand the private and family life of a little boy who had had his whole world turned upside down by the death of his older brother allegedly at the hands of his mother. He faced having to live and go to school with daily publicity about the intimate details of his family life over the several months while his mother was being tried for his brother’s murder. That publicity would include the names and photographs of both his mother and his brother from which he could readily be identified. There was psychiatric evidence of the harm which he was likely to suffer as a result. This would include not only the further increase in the already much heightened risk of mental illness in adulthood but also the harm to his relationship with his mother, which on any view was important to his continuing health and development. On the other hand was the public interest in the free reporting of murder trials. This is not only important in itself, as a manifestation both of freedom of expression and freedom to receive information. It is also an essential component in a fair trial (albeit one which this accused was more than willing to relinquish for the sake of her surviving son) and in securing that justice is done in the open and not in secret. So that the public can have confidence in the system both in general and in the particular case. Although it was held by the Court of Appeal that upheld the decision of the High Court judge holding that “the judge had the issues that he was required to balance well in his mind and had given a clear indication that he had considered that the interference with
the child's rights under art 8 was proportionate in the light of public interest and the rights of the press under art 10."

and for the same reason the House of Lords [2004] UKHL 47 dismissed the appeal – it has been accepted by all level of the courts that the provision of art. 8(1) ECHR was rightfully engaged in the application for the restriction of publication.

[31] (1948) 65 R.P.C. 203
[34] That this is the law is shown by two passages in the judgments of the Court of Appeal in *Attorney-General* v. *Guardian Newspapers Ltd.* (No. 2) [1988] 2 W.L.R. 805 the *Spycatcher* case, Sir John Donaldson M.R. said, at p. 868: "As a general proposition, that which has no character of confidentiality because it has already been communicated to the world, i.e., made generally available to the relevant public, cannot thereafter be subjected to a right of confidentiality... However, this will not necessarily be the case if the information has previously only been disclosed to a limited part of that public. It is a question of degree." Bingham L.J. said, at p. 903. "The information must not be 'public knowledge' (*Seager* v. *Copydex Ltd.* [1967] 1 W.L.R. 923, 931G per Lord Denning M.R.), nor in the public domain: *Woodward* v. *Hutchins* [1977] 1 W.L.R. 760, 764D *per* Lord Denning M.R. To be confidential information must have what Francis Gurry recently called the basic attribute of inaccessibility: see Gurry, Breach of Confidence (1984), at p. 70.

[37] This requirement, however, has been relaxed if not dispensed with, see the text of footnote 43 and the accompanying text thereto.


[40] *Ibid*.
[42] See *Re Roddy* footnote 2 above.

[43] Eg., *Attorney-General* v. *Guardian Newspaper Ltd* (No. 2) [1990] 1 A.C 109 at 281 and *Hellewell* v. *Chief Constable of Derbyshire* [1995] 1 W.L.R 804 at 807. Most recently in *Wainwright and Another* v. *Home Office* [2003] UKHL 53 in interpreting the judgment of Sedley L.J. in *Douglas v Hello! Ltd* [2001] QB 96, Lord Hoffmann said that to the judgment is in effect excludes the need to prove the existence of trust or relationship based on confidence which otherwise is essential in an action for breach of confidence (*Wainwright* at paras 29 and 30). See, however, El Islamy, Hurriyah, “Wainwright: Does not an individual have a right to be let alone” due to be published on Obiter, March 2005 issue (both online and hard copy versions).

[47] See for examples: *Malone v. United Kingdom* (1984) 7 EHRR 14; *Kaye v. Robertson* [1991] FSR 62; *Wainwright and Another v. Home Office* [2003] UKHL 53, etc. A convenient summary of these cases is to be found in Gavin Phillipson's valuable article 'Transforming Breach of Confidence? Towards a Common Law Right of Privacy under the Human Rights Act' (2003) 66 MLR 726, 726-728 where in the last page it was concluded that “[b]reach of confidence is being used today as a privacy remedy; frequently, but in many cases, not effectively.”


[49] [2004] UKHL 22