Summary Article: Internet, Regulation and Censorship
From Encyclopedia of Applied Ethics

The Internet has become a central part of human existence. It provides a universal means of exchanging information. Its unregulated nature means that it can be used for either the transmission of illegitimate information for nefarious purposes or for transmission of information which is deemed to be politically unacceptable.

This article considers the issues around the regulation of the Internet and explores the ethical and legal issues around the difference between regulation and censorship.

Censorship
Freedom of Expression
Internet
Phishing
Pornography
Regulation
Spam
Standards
World Wide Web

The Internet
The Internet has its origins in a number of developments in the history of computer science. Arguably, the first reference to the concept in an operational context is by J.C.R. Licklider, who in 1962 wrote memos about his concept of an Intergalactic Network concept, where everyone on the globe is interconnected and can access programs and data at any site from anywhere. He was already talking to a network of researchers across the United States. In October 1962, he became the first head of the computer research program at ARPA, which he called the Information Processing Techniques Office (IPTO). In the same year, Leonard Kleinrock completed his Ph.D. studies on queuing theory in communication networks.

In 1963, a joint industry-U.S. government committee developed the first universal standard for computers, the American Standard Code for Information Interchange (ASCII), which allowed machines from different manufacturers to exchange data.

In 1967, the plan for ARPAnet was published, and the first transmission via the ARPAnet (which crashed!) occurred in 1969. The second was successful. Further development led to the File Transfer Protocol (FTP) in 1971 and the first public demonstration in 1972. The same year the ubiquitous convention of user@host was introduced as part of the first e-mail application designed to transmit over the ARPAnet. However, this was not to become a worldwide standard for nearly two decades.

In 1973, Kahn and Cerf presented their Transmission Control Protocol to allow ARPAnet to talk to other networks using different interfaces. ARPA became DARPA to reflect its defense application. At this
time, the first incarnation of Ethernet was developed and shown by Xerox at Palo Alto. By 1978, the term 'Internet' was introduced to represent the collection of networks that could talk to each other.

By 1983, the Internet had grown to the point where a new address system was needed and the Domain Name System was introduced.

In 1989, Tim Berners-Lee proposed a hypertext system that would run across the Internet on different operating systems. This became the World Wide Web. In 1992, Mosaic, the first Internet browser, was developed. By this time, all the key elements that made up the modern Internet were in place.

In December 2008, the number of unique users of the Internet exceeded 1 billion, with 41% from Asia, 28% from Europe, and 18% from North America.

From a technological perspective, the Internet is a highly regulated environment. Its development is the development of a series of common standards that facilitate communication. A modern network is defined in terms of seven layers of standards defined within the OSI 7-layer model. At each level, the operation must be carried out according to a standard protocol so that the information received is able to be reconstructed in the form it was transmitted (Table 1).
Table 1 The seven layers of the OSI Network model

<table>
<thead>
<tr>
<th>Layer</th>
<th>What it does</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>This layer supports application and end-user processes. Everything at this layer is application-specific. Telnet and FTP are applications that exist entirely in the application level.</td>
</tr>
<tr>
<td>Presentation</td>
<td>This layer provides independence from differences in data representation (e.g., encryption) by translating from application to network format and vice versa. The presentation layer works to transform data into the form that the application layer can accept. This layer formats and encrypts data to be sent across a network, providing freedom from compatibility problems. It is sometimes called the syntax layer.</td>
</tr>
<tr>
<td>Session</td>
<td>This layer establishes, manages, and terminates connections between applications. The session layer sets up, coordinates, and terminates conversations, exchanges, and dialogues between the applications at each end. It deals with session and connection coordination.</td>
</tr>
<tr>
<td>Transport</td>
<td>This layer provides transparent transfer of data between end systems, or hosts, and is responsible for end-to-end error recovery and flow control. It ensures complete data transfer.</td>
</tr>
<tr>
<td>Network</td>
<td>This layer provides switching and routing technologies, creating logical paths, known as virtual circuits, for transmitting data from node to node. Routing and forwarding are functions of this layer, as well as addressing, Internet working, error handling, congestion control, and packet sequencing.</td>
</tr>
<tr>
<td>Data link</td>
<td>At this layer, data packets are encoded and decoded into bits. It furnishes transmission protocol knowledge and management and handles errors in the physical layer, flow control, and frame synchronization. The data link layer is divided into two sublayers: The Media Access Control (MAC) layer and the Logical Link Control (LLC) layer. The MAC sublayer controls how a computer on the network gains access to the data and permission to transmit it. The LLC layer controls frame synchronization, flow control, and error checking.</td>
</tr>
<tr>
<td>Physical</td>
<td>This layer conveys the bit through the network at the electrical and mechanical level. It provides the hardware means of sending and receiving data on a carrier, including defining cables, cards, and physical aspects. Fast Ethernet, RS232, and ATM are protocols with physical layer components.</td>
</tr>
</tbody>
</table>

Regulatory Bodies Associated with the Internet and Their Purpose

World Wide Web Consortium

There are a number of bodies that seek to regulate the Internet and its applications, such as the World Wide Web Consortium (W3C), whose purpose is to design and maintain technical standards. The W3C is an international community that develops standards to ensure the long-term growth of the Web. It is a not-for-profit organization that defines a range of standards. The most significant is the HTML standard, which defines how Web pages should be written and interpreted by browsers. If there is a mismatch, then the page will not appear on the screen as the author intended.

A growing area of activity for the W3C is ensuring that Web pages are accessible to all, including those using special aids to access pages because of visual impairments. This is significant because it moves
the role of W3C beyond the purely technical to the area of embodying values. For example, Sir Tim Berners-Lee, inventor of the World Wide Web and W3C Director, argues that “The power of the Web is in its universality. Access by everyone regardless of disability is an essential aspect.” (W3C (2010) World Wide Web consortium website)

This principle drives W3C’s work to make the Web accessible to all. According to W3C:

*The Web is fundamentally designed to work for all people, whatever their hardware, software, language, culture, location, or physical or mental ability. When the Web meets this goal, it is accessible to people with a diverse range of hearing, movement, sight, and cognitive ability.*

*Thus the impact of disability is radically changed on the Web because the Web removes barriers to communication and interaction that many people face in the physical world. However, when websites, web technologies, or web tools are badly designed, they can create barriers that exclude people from using the Web.*

W3C has created the Web Accessibility Initiative (WAI) to lead the Web to its full potential of being accessible, enabling people with disabilities to participate equally on the Web.

**ICANN**

ICANN was formed in 1998. It is a not-for-profit public-benefit corporation with participants from all over the world dedicated to keeping the Internet secure, stable, and interoperable. Its role is to define and regulate every address on the Internet.

To reach any other person on the Internet, one must provide an address to the computer: a name or a number. That address must be unique, so computers know where to find each other. ICANN coordinates these unique identifiers across the world. Without that coordination there would not be one global Internet.

Until 2009, ICANN was established by the U.S. government and until 2009 was under close U.S. government control through periodically signed accords – known collectively as the Joint Project Agreement (JPA) – with the U.S. Commerce Department’s National Telecommunications and Information Administration. These papers meant that the U.S. government was responsible for reviewing the work of the body.

This drew criticism from other countries and groups such as The European Commission, which argued that previous arrangements failed to reflect the global nature of the modern Internet.

In 2009, the U.S. government relaxed its control over how the Internet is run and signed a four-page affirmation of commitments with the ICANN, giving the body autonomy for the first time. Affirmation of commitments are brief documents that are now reviewed by the global Internet community.

In addition, independent review panels, including representatives of foreign governments, now specifically oversee ICANN’s work in three specific areas: security, competition, and accountability.

However, the U.S. government will still have a strong role in regulation. They will retain a permanent seat on the accountability panel. ICANN also has a separate agreement with the United States – to run the Internet Assigned Numbers Authority (IANA) – that expires in 2011.

**The Nature of the Problem**

https://search.credoreference.com/content/topic/internet_regulation
There is a paradox at the heart of the Internet. The Internet technical platform is a highly controlled and regulated environment. It is almost certainly the largest example of a commonly agreed technical solution that depends upon everyone using the same technical standards, with 1 billion unique users and probably another billion with access to it.

The content expressed through Web pages, e-mails, and increasingly social networking sites built on this platform is often perceived to be a wildly unregulated environment, portrayed as a kind of virtual Wild West, with everyone joining in the gold rushes of the dot-com boom and e-commerce, showing little respect for the rules. The popular media emphasizes the nefarious purposes to which it is put, including financial scams, pornography, terrorism, and unreliable medications to improve sexual performance. Almost without exception, when a major scandal, for example a network of pedophiles or a terrorist group, is uncovered, they will have used the Internet in some form to communicate. They will also certainly have used other means such as telephones, mobile and fixed line, but these seem to attract less negative attention. The Internet is often implied to be encouraging people to commit crimes, for example the Sun headline from 14 October 2009: “A PREGNANT mother of eight who is the latest alleged pervert seized over a Facebook paedophile ring is a SECOND nursery nurse, The Sun can reveal.” According to the security firm Symantec, which obviously has a vested interest in talking up the story, spam e-mails now account for 86% of global e-mails (October 2009). Many of these spam e-mails are designed to extract personal details in order to facilitate identity theft in the practice known as phishing.

One of the standard responses to this is the call for the content of the Internet to be more closely regulated to reduce the risk of harm. The UK suggests that regulation can only be a partial solution to spam e-mails.

According to advice from the UK Information Commissioner’s Office, The Privacy and Electronic Communications Regulations lay down rules for organizations sending unsolicited marketing by electronic means. The rules are different depending whether the recipient is an individual subscriber or a corporate subscriber. The regulations do not specifically deal with the worldwide problem of spam, and only cover e-mails sent from within the EU.

The regulations say that organizations must have prior consent to send unsolicited marketing material by electronic mail to individual subscribers, unless they have obtained the details during the course of a sale, or negotiations toward one, and they give you the opportunity to object in every message. If you are an individual subscriber receiving unsolicited marketing by electronic mail, and the organization has not stopped even though you have tried to opt out, you can complain to the Information Commissioner.

If you are a corporate subscriber the prior consent rule does not apply. Marketing communications should still identify the sender and provide a valid address. Depending on the information the company holds about you, a corporate subscriber may also have rights under Section 11 of the Data Protection Act 1998.

There are practical steps that can be taken to reduce spam. Arguably, all users of e-mail have an interest and a duty in taking steps to reduce spam. The official advice includes the following:

Be careful who you give your e-mail address to.

Consider having separate personal and business e-mail addresses.
Choose an e-mail address which is difficult to guess.

Do not advertise your e-mail address.

Check privacy policies and marketing opt-outs carefully.

Do not reply to e-mails unless you are familiar with and trust the sender.

Do not click on the adverts in spam e-mails.

Use a spam e-mail filter on your computer.

Keep your systems well maintained.

Check privacy policies and marketing opt-outs carefully.

According to the UK Broadcasting Standards Commission, as far back as 1999 almost three-quarters of the population were calling for some form of Internet regulation. Although much regulation already occurs at a local level through access controls and moderation of content, 10 years later, little progress has been made nationally or globally. Regulation of content of the Internet raises a number of difficult questions:

Who should be the regulator?

What criteria should be used to judge what is suitable and what is not?

There is a third issue, which is how might this be achieved, but in reality, most of the mechanisms are already in place. Because the Internet is still largely a text-based medium, it automatically creates its own audit trail. If you are in any doubt about the extent to which material placed online is permanent, visit www.archive.org and try the Wayback tool.

Common methods used to prevent inappropriate access include:

- IP address blocking. Access to a certain IP address may be denied. If the target website is hosted in a shared hosting server, all websites on the same server will be blocked. This allows administrators to create blacklists of sites. This may be used by schools to prevent children accessing inappropriate material or employers to prevent employees accessing frivolous sites during work hours.

- DNS filtering and redirection. This prevents access by stopping the resolution of domain names that contain key phrases or words. This can be relatively easily circumvented by typing the IP address instead of the domain name in a Web browser.

- Uniform Resource Locator (URL) filtering. This is similar to the above, but involves scanning the requested URL string for target keywords regardless of the domain name specified in the URL.

- Packet filtering. This technique measures the frequency of keywords and terminates packet transmissions when a certain number of controversial keywords are detected.

- Web feed blocking. Where Web feeds or blogs are deemed to be inappropriate, incoming URLs starting with the words ‘rss,’ ‘feed,’ or ‘blog’ are blocked. However, blocking can have unexpected consequences when offensive strings form part of larger words that are perfectly innocent (a town in Lincolnshire is alleged to be blocked from many searches as it contains within its name a
four-letter group that forms a word deemed to be offensive) and every blocking strategy tends to lead to a counter-strategy from those engaged in inappropriate behavior.

The Need for Regulation

One of the key drivers for Internet regulation is child protection. The World Wide Web has huge educational potential and children are enthusiastic early adopters of technology. In recent years, there has been a sea change in the use of new technologies, especially by girls, as technology has moved out of the hands of geeks and is now a key part of children's social fabric. This increasing usage has led to growing fears regarding the presence of content that could have a harmful effect on children using the Internet, especially sex, nudity, violence, and language, and increasingly inappropriate social contacts including cyberbullying by peers to grooming by predatory adults.

These concerns have led to a number of international initiatives to coordinate hotlines for reporting illegal or harmful material by nongovernmental groups such as the Internet Watch Foundation which is leading some of this work. Multilateral organizations such as the United Nations and Interpol have organized many international conferences to improve the policing of the Internet for the purposes of child pornography and child prostitution.

In the United States, the Recreational Software Advisory Council (RSAC) devised a content rating and filtering system in 1996, largely in response to federal government attempts in the United States to regulate indecent content online. The RSAC system used a scale of 0 to 4 in four categories: sex, nudity, violence, and language. The RSAC was reformed as the Internet Content Rating Association (ICRA) in 1999, and its work is now part of The Family Online Safety Institute.

One of the challenges regarding the Internet is its global nature. Effective regulation would require international cooperation. Different nations have different cultural norms about moral issues, especially about sex. Some countries resent the perceived dominance of American culture and the English language.

French language protagonists have long complained about what they see as an American invasion of their culture (particularly in films, music, and television). For them, the Internet is simply the latest threat and they argue that current laws, aimed at preserving the French language, should apply to Internet sites as well. However, this is anathema to those who argue that as the Internet is accessed by people around the world, to impose a language on it would be nonsense and could lead to French culture being further marginalized.

E-commerce is still growing rapidly. International e-commerce is seen by some as a threat and by others as an opportunity. It is as easy to buy from a website based in China or the United States as from one based along the street, but trade agreements as well as border and customs controls have struggled to keep up with technological possibilities, leading to barriers to legitimate trade and ineffective policing of smuggling in goods, people, and illegal substances.

The Problem of Censorship

Many people who favor regulation would oppose censorship. And yet the dividing line between censorship and regulation is unclear. At its crudest, regulation becomes censorship when it prevents activity that I think is either beneficial or at least not doing harm. Different countries have adopted different approaches to regulating the Internet and some of these may be regarded as either
censorship or more subtle oppression, where communications are allowed to proceed but are closely monitored for evidence of criminal, terrorist, or subversive activity. Again, if we view the alleged activity as criminal or terrorist we may approve of such actions, but if we regard it as antisubversive and carried out by an oppressive regime, we may regard it as unacceptable.

Consider Singapore. It is a country which has widely embraced the Internet and is at the forefront of providing online access to public services and government agencies. However, the Internet is subject to strong government control. Singapore’s government-run Media Development Authority maintains a confidential list of blocked websites that are inaccessible within the country. The Media Development Agency exerts control over Singapore’s three ISPs to ensure that blocked content is entirely inaccessible.

External agencies judge the supervision to be largely benign. For example, a report to the New South Wales Parliament in Australia found that while the Australian Communications and Media Authority (ACMA) has the power to impose sanctions, including fines, on licensees who contravene the Code of Practice, they take a light-touch approach in regulating services on the Internet. For example, licensees (Internet content providers and Internet service providers) found to be in breach of regulations will be given a chance to rectify the breach before the Authority takes action.

Prohibited material is defined in the Code of Practice and appears to involve material deemed unsuitable for adults by the Singaporean government. It does not appear to cover information unsuitable for minors, nor does it contain a requirement that websites attempt to restrict access to such material to adults. Briefly, prohibited material is that which is deemed “objectionable on the grounds of public interest, public morality, public order, public security, national harmony, or is otherwise prohibited by applicable Singapore laws.” The stated factors to be considered in determining what is prohibited material indicate this includes material of a pornographic nature; advocacy of “homosexuality or lesbianism”; depictions of “detailed or relished acts of extreme violence or cruelty,” and material that “glorifies, incites or endorses ethnic, racial or religious hatred, strife or intolerance.” An additional factor is “whether the material has intrinsic medical, scientific, artistic or educational value.” They conclude that users in Singapore have access to all material available on the Internet, with the exception of a few high-impact illegal websites whose content on the Internet is not pre-censored.

Contrast this with the twelve countries that were listed in 2009 on a blacklist published annually by Reporters sans frontières, RSF, a Paris-based international nongovernmental organization that advocates freedom of the press. The twelve countries were Burma, China, Cuba, Egypt, Iran, North Korea, Saudi Arabia, Syria, Tunisia, Turkmenistan, Uzbekistan, and Vietnam.

In some cases, RSF reports that censorship is clandestine, in other cases, it is overt. For example, China allegedly seeks to present an open view to the world: China unquestionably continues to be the world’s most advanced country in Internet filtering. The authorities carefully monitor technological progress to ensure that no new window of free expression opens up.

They report that much of China’s effort is concentrated on blogging sites and that China’s blog tools all include filters that block what are deemed subversive word strings. Furthermore, they report that companies operating these services, both Chinese and foreign, are pressured by the authorities to control content.

UK politicians have criticized Western IT companies for collaborating with state censorship of the Web
in China. The companies accused include Microsoft, Google, and Yahoo, and their conduct has been described as morally unacceptable by the Commons Foreign Affairs Committee.

In 2007, Yahoo shareholders rejected plans for the company to adopt a policy that opposes censorship on the Internet. Proposals to set up a human rights committee to review its policies around the world, specifically in China, were also heavily defeated. The policy was in response to the company making private e-mails available to the Chinese authorities, leading to the prosecution and imprisonment of political dissidents, but Yahoo insists it must comply with local laws in areas where it operates.

Google adopted an agreement with the Chinese government to restrict access to certain sites in order to continue operating in the country. Nevertheless in 2009, Google’s international and Chinese websites were blocked periodically in many parts of China, as has the Gmail service.

RSF contrasts the Chinese situation with that of a country like Saudi Arabia. They report that unlike China, where website blocking is disguised as technical problems, Saudi Arabia’s filters clearly tell Internet users that certain websites are banned. Saudi Arabia is an Islamic country, so much of the censored content is focused around pornography, which is contrary to the religious views of the country. This is also true of the censorship around homosexuality, which is illegal in the country. RSF reports that they also block material on overtly political grounds such as opposition websites and Israeli publications.

Surveillance of the Internet often increases in the aftermath of high-profile events. Thus, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (aka USA PATRIOT Act) of 2001 gave the U.S. government sweeping powers to search telephone and e-mail communications and to access medical, financial, and other records. It also eased restrictions on foreign intelligence gathering within the United States and increased the government’s powers to monitor the activities of immigrants. At the same time, it expanded the definition of terrorism to include domestic terrorism, thus enlarging the number of activities to which the Act’s expanded enforcement powers could be applied. While it was originally passed with a wide margin in the aftermath of 9/11, it was designed to be time-limited with the provisions expiring in 4 years. However, these emergency measures were largely retained in revised legislation in 2005 and 2006, and key powers seem likely to be retained by the Obama administration.

Similar powers were enacted by the UK government in its Prevention of Terrorism Act, but at the time of writing, e-mail interception and phone tapping are not admissible as evidence in a British court.

One Man’s Regulation Is Another Person’s Censorship

The dividing line between legitimate regulation and censorship is not as clear as we might wish. It is more complicated both legally and ethically when dealing with a global entity such as the Internet. Berners-Lee’s aspiration that the power of the Web is in its universality makes it in many ways the ultimate symbol of free speech. When this freedom is used to achieve goals that we support it is very attractive, but when used for purposes we regard as harmful, it becomes much more harmful. In some cases, it may even be in danger of self-destruction. If spam levels rise even higher and approach 90%, 95%, 99%, then a tipping point will be reached and legitimate users will reduce their usage. At this point, the percentage of spam rises by default, and this could lead to a doomsday scenario.

However, in most cases there is a continuum between legitimate and illegitimate use and the case for
regulation and censorship is where you draw a dividing line between legitimate and illegitimate use. This article will consider the issues around that dividing line in key areas of the Internet.

**Sex and Pornography**

Pornography is the spam of Internet searches. Although the growth of social networking has dethroned searching for pornography as the most common Internet activity, it is still reported to account for about 10% of all searches, down from around 20% a decade ago. Therefore, the fear that such traffic will clog up the Internet appears unfounded.

The second problem is the harm that may follow from users accessing the material. Some material will be equivalent to that stocked on the top shelf of the local newsagent. When viewed by appropriate adults, this appears to be no more harmful than that available elsewhere.

The greater harm arises when more serious material is available or material is made available to inappropriate groups such as children. A number of measures are in place to prevent this. Search engines use filters to prevent accidental access to offensive material. Studies by the Communicable Diseases Center show these to be largely effective and to be relatively free of undesirable side effects of blocking access to legitimate health advice.

However, all of these filters can be switched off. Specific software can be purchased to prevent children accessing inappropriate material, and environments such as schools will provide external access controls.

One of the areas where the Internet has had bad press is in the area of child pornography. Even in this area, there are some ambiguities. Production and possession of child pornography, if it is illegal and immoral in a society, is still illegal and immoral when associated with the Internet. There are some practical issues: the Internet offers a means of distribution that can help spread inappropriate material more easily. The additional dilemma of principle arises from the global nature of the Internet. The age at which young people are deemed to be sexually mature varies from society to society. Thus, a pornographic representation of a 15-year-old girl would be deemed exploitative and illegal in most Western societies. In some other societies, she could be legitimately married with children. Thus, such an image could be made in a society where it was perfectly legal. At what point does it become inappropriate? The point where it is uploaded to the Internet with the purpose of being viewed in a situation where it is illegal so to do? The point where it is accessed via the Internet for illegal purposes?

Tensions rise within a global system where local customs differ. Saudi Arabia is described as censoring the Internet for, among other reasons, censoring sites on homosexuality. While Western liberal democracies would defend the equality of treatment of all groups irrespective of sexual orientation, some members of Christian religious movements in the West would share the view of the Saudis that this material is inappropriate and should be banned. While those living in a liberal democracy enjoy the right to at least debate the issue, attitudes to censorship of material about abortion and evolution in the United States suggest that given the opportunity, these people would ban such material without a qualm in the alleged interests of protecting their children, as happened over evolution in the Stopes trial of 1925, and much more recently over the teaching of intelligent design in American schools.

The unique aspect of all these freedom of speech debates arising from the Internet is its global nature.

[https://search.credoreference.com/content/topic/internet_regulation](https://search.credoreference.com/content/topic/internet_regulation)
Health Advice and Online Pharmacies

Another media concern is the growth of cyberchondria: the phenomenon of patients arriving at the doctor’s surgery having self-diagnosed from the Internet. This is accompanied by the growth of unlicensed pharmacies.

There are many sites giving health advice on the Web from a wide variety of sources. They may be provided by health care organizations such as the NHS in the UK patient groups, drug companies, or people pushing unproven treatments or simply trying to obtain money from sick or distressed patients for counterfeit or placebo drugs.

In the UK, the growth of these sites accompanied an erosion in confidence in the medical profession following scandals in Bristol, Liverpool, Kent, and Hyde. Although each of these situations is different, they led to a cumulative erosion in confidence in doctors and encouraged patients to seek additional sources of information for reassurance.

The challenge for governments is how far to regulate these websites, and for individual professionals to decide how far they should engage with them. Once again, the global nature of the Internet means that it is very difficult to regulate these sites. An attempt to do so could be seen as an attempt to censor information that might suggest that in a publicly funded system such as the NHS, the government is trying to block access to information on new treatments that are expensive but effective.

A number of approaches are possible to mitigate potential harm:

  Establish reputable sites. This has been done in the UK with sites such as NHSDirect Online. These may contain reputable information but still have risks associated with them because what a patient does with the information cannot be controlled.

  Educate patients. There have been a number of initiatives designed to educate patients on how to spot a website that is likely to be trustworthy and manage the information obtained in a responsible manner.

  Encourage clinicians to use reputable sites as part of their consultation and encourage them to facilitate effective use of health information websites.

  Establish a quality accreditation scheme where sites may apply to be given accredited status. The problem is to establish a regulatory process that is credible with patients and professionals.

Online pharmacies are a growth area. They are less popular in the UK than other countries where the cost of medicines is higher for patients. The retail pharmacy sector in the UK and many other countries is highly regulated. Online pharmacies are not so highly regulated, and it is much harder to spot a rogue online pharmacy.

Some of the apparently most reputable online pharmacies provide a user review system where users are invited to rate the efficacy of both the site and the medication, for example Pharmacy Reviewer. This is either the height of Internet democracy or a bizarre example of data of very dubious relevance to a specific user presented in a misleadingly authoritative manner. To one used to the NHS system, this appears to be fraught with risk, but in the recent debate in the United States over health care choices, it has been obvious that different views exist in different cultures. Once again, the Internet
seeks to provide a global solution, although it may conflict with local norms and values.

In the UK, probably the largest area of online pharmacy is in the provision of impotency medications. A significant proportion of spam e-mails offer Viagra or similar medications. Again, there are significant risks arising from counterfeit or impure medications, plus the risks of side effects when the patient has not been advised and checked out by a health care professional. However, these advertisements are so widespread that regulation or censorship beyond local precautions, for example, classifying all e-mails about Viagra as spam, are likely to prove ineffective, and the above generic health information strategies are the most likely to be effective.

**See Also**
Censorship; Computer and Information Ethics; Privacy, Ethics of.

**Relevant Websites**
The online journal Studies in Ethics Law and Technology [http://www.bepress.com/selt](http://www.bepress.com/selt)
The author’s website with links to further resources [http://www.alangillies.com](http://www.alangillies.com)
The website of the World Wide Web (W3C) consortium [http://w3.org](http://w3.org)

**Further Reading**
- A. Murray The Regulation of Cyberspace 2006 Routledge-Cavendish Abingdon.

**Glossary**

**Censorship**
The institution, system, or practice of reading communications and deleting or preventing access to material considered sensitive or harmful, especially when exercised repressively. It has its origins in the name of one of two magistrates of early Rome acting as census takers, assessors, and inspectors of morals and conduct.

**HyperText Markup Language (HTML)**
The publishing language of the World Wide Web. HTML 4 is an SGML application conforming to International Standard ISO 8879. For Web pages to be rendered correctly, the page must be correctly written in HTML, and the browser program must be capable of interpreting the version of HTML in which the page is written.

**Internet**
The Internet is a massive network of networks, a networking infrastructure. It connects millions of computers together globally, forming a network in which any computer can communicate with any other computer as long as they are both connected to the Internet. Information that travels over the Internet

[https://search.credoreference.com/content/topic/internet_regulation](https://search.credoreference.com/content/topic/internet_regulation)
does so via a variety of languages known as protocols.

**Phishing**
The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise. The purpose of phishing is to scam the user into surrendering private information, in the pursuit of identity theft. The e-mail directs the user to visit a website where they are asked to update personal information such as passwords and credit card, Social Security, and bank account numbers, which have already been collected by the legitimate organization. The website logs any details and transmits to the criminals behind the site.

**Regulation**
The process of imposing authoritative rules dealing with details or procedures issued by an executive authority or regulatory agency of a government with the goal of preventing inappropriate, unsafe, or illegal actions.

**Spam**
Electronic junk mail or even more generally any unsolicited e-mail. Genuine spam is generally e-mail advertising for some product sent to a mailing list or newsgroup, notoriously linked to medications to enhance sexual potency or financial scams. There is some debate about the source of the term, but the generally accepted version is that it comes from the Monty Python “Spam” song.

**World Wide Web**
The World Wide Web, or simply Web, is a way of accessing information over the medium of the Internet. It is an information-sharing model that is built on top of the Internet. The Web uses the HTTP protocol, only one of the languages spoken over the Internet, to transmit data. Web services, which use HTTP to allow applications to communicate in order to exchange business logic, use the Web to share information. Users access information using computer applications known as browsers such as Internet Explorer or Firefox to access Web documents called Web pages that are linked to each other via hyperlinks. Web documents may also contain images, graphics, audio, text, and video.

A. Gillies

School of Public Health and Clinical Sciences, Preston, UK

**APA**

**Chicago**

**Harvard**

**MLA**


Copyright © 2012 Elsevier, Inc. All rights reserved.