silenced

an international report on censorship and control of the Internet

By Privacy International and the GreenNet Educational Trust

Supported by the Open Society Institute (OSI)
http://www.soros.org/

September 2003

www.privacyinternational.org

www.greennteducationaltrust.org.uk

Publishing License

Cover design by nani buntarian
Layout by Tristram Ariss, +44 1227 713535

Printed by Setline Data Ltd
setlinedata@aol.com
tel: +44 207 232 0446
fax: +44 207 740 2401

September 2003

This book is also available online at:
www.privacyinternational.org/survey/censorship

About the Organisations

About Privacy International
Privacy International (PI) was formed in 1990 as a watchdog on surveillance by governments and corporations. The organisation is based in London, England, and has an office in Washington, DC. PI has conducted campaigns throughout the world on issues ranging from wiretapping and national security activities, to ID cards, video surveillance, data matching, police information systems, and medical privacy. Details of the organisation's publications, reports and conferences can be found at:
www.privacyinternational.org

About GreenNet Educational Trust
GreenNet Educational Trust (GET) was established to promote the advancement of education to support, encourage and promote research into the use of computers, electronic communications and information technology by the general public. It is the parent company of GreenNet Limited, a not for profit Internet Service Provider dedicated to supporting and promoting groups and individuals working for peace, human rights and the environment through the use of information and communication technologies (ICTs). More information about our work can be found at:
www.greenneteducationaltrust.org.uk

Methodology

The production of this report has involved around fifty experts and advocates from around the world. Most have been engaged in the task of researching and writing specific country reports. These reports have been authenticated and augmented by regional editors. The report as a whole has been assessed by a team of editors from Privacy International and GreenNet Ltd in London.

We have been anxious to ensure that anecdotal evidence from the front line was incorporated into the report, but have also used traditional research benchmarks in the creation of the report's contents. Wherever possible the authors and editors have cited studies, legislation and case law relevant to each country and region.

It is important to note that the regional reports were written as assessments of trends that became visible when analysing country studies. As such, many of the regional analyses refer to national studies within the report and do not therefore contain separate bibliographical references. Because different countries' use of the Internet is affected heavily by specific national priorities, there are different emphases in the reports that recognise the diverse social, economic and political conditions in which the Internet is being used. We have attempted to be as comprehensive as possible in our choice of countries, and will progressively expand the number of national reports in future editions.

Acknowledgements

The research, writing and production of this report was undertaken primarily by David Banisar, Gus Hosein and Simon Davies (Privacy International), Heather Ford and Karen Banks (GreenNet Educational Trust) and Wendy Grossman.

Regional overviews were written by Ernesto Hilario (Asia), Heather Ford (Africa), Wendy Grossman (Europe), Ahmed El Gody, Modern Sciences and Arts University, Egypt (Middle East), Pablo Palazzi (Latin America) and Simon Davies (North America).

We would like to thank all of those who contributed to the writing and research of the country reports:

Ahmed El Gody, Modern Sciences and Arts University (Bahrain, Jordan, Qatar, Saudi Arabia); Alexander Schirge (Germany); Andrea Monti (Italy); Andriy Pazyuk, Privacy Ukraine (Ukraine); Big Brother Awards (Switzerland); Bretton Vine, Future Foundation (South Africa); Carlos G Gregorio (Costa Rica, Uruguay); Christoph Mueller (Switzerland); David Banisar (Council of Europe, UK); David Casacuberta Sevilla (Spain); Erich Moechel (Austria); Erick Iriarte Ahon, Alfa-Redi (Peru); Frederick Noronha (India); Heather Ford (Egypt, Kenya, Zimbabwe); Marie-Helene Mottin Sylla (Senegal); Nick Luethi (Switzerland); Irene Graham, Executive Director, Electronic Frontiers Australia Inc. (Australia); Jason Young, Privaterra (Canada); Jens Franz (Singapore, Thailand); Lishan Adam (Ethiopia); Marek Tichy, Econnect (Czech Republic); Mário Antônio Lobato de Paiva (Brazil); Meryem Marzouki, Imaginons un réseau Internet solidaire, IRIS (France); Nnenna Nwakanma (Cote d'Ivoire); Pablo Palazzi (Argentina); Polly Gaster, Eduardo Mondlane University Informatics Centre, CIUEM (Mozambique); Rikke Frank Joergensen, The Danish Institute for Human Rights (Denmark); Sergei Smirnov (Russia); Swiss Internet User Group SIUG (Switzerland); Tess Hocson, WomensHub (Philippines); Wendy M. Grossman (Belgium, Burma, China, EU, Morocco, Spain, UAE, UK, US, Uzbekistan); Yaman Akdeniz, Cyber-Rights & Cyber-Liberties (Turkey); YK Chang (South Korea); and Zoltan Galantai (Hungary).

Thanks also to the following:

Alvar Fruede (Germany); Anriette Esterhuysen, APC (South Africa); Bev Clark, kubatana.net (Zimbabwe); GreenNet Ltd Staff; Irene Petras, Zimbabwe Lawyers for Human Rights (Zimbabwe); Ian Brown (UK); Jagdish Parikh (India); Leila Hassanin (Egypt); Leo Fernandez (India); Muriuki Mureithi (Kenya); Okoth F. Mudhai (Kenya); Ralf Bendrath (Germany); Rick Abbey (UK); Sarah Masters (UK) and Vsevolod Paevsky (Uzbekistan).

Thanks also to Marc Rotenberg and the Electronic Privacy Information Center for their continued encouragement, leadership and support.

We would like to express our gratitude to the Open Society Institute for its generous financial support for this project.

Dedicated to the memory of

W.J. (Bill) Reddin

Friend and Visionary

Foreword

The Internet is living through interesting times. No communications and information medium in history has endures such a continued and varied assault on its functioning and its infrastructure. This is particularly true since the 11th September 2001. Few governments have resisted the opportunity in the past two years to enact laws restricting a range of civil rights. The Internet is seen by many of these governments as a potential threat to security and authority.

The backlash is predictable. Governments and their agencies have traditionally viewed new technologies with suspicion, arguing that their presence can disturb the hard-won "balance" of rights and responsibilities, in the same way that large companies have traditionally viewed any new media as a threat to the balance of their markets. Unconventional forms of publishing and speech challenge conventional ways of conducting business and governing society. Historically, only an exceptionally small and forward-looking group of companies and government agencies take advantage of new media. Others resist their implementation, and attempt to use legal mechanisms to frustrate access to such technologies and techniques.

That scenario applies even more so in the legal and constitutional battles to protect civil rights. While paying lip service to personal freedoms, the leaders of the democratic world have affirmed with uncharacteristic harmony that the pursuit of a safer society must prompt a reassessment of individual liberties and privacy. In its most blatant manifestation, this will result in a substantial increase in the right of the state to place controls on all citizens, shifting the default in favour of comprehensive surveillance over the population. Technology is at the same time the culprit and the saviour.

The events of September 11 have provided a springboard for measures that in another era might have been abandoned as unworkable or found to be unacceptably heavy-handed. Freedom of Information, privacy, on-line free speech and security of communications are likely to buckle under the pressure of a regulatory zeal rarely seen in peace-time.

In conducting the research for Silenced we were confronted with a number of difficult questions. One of the most contentious and disconcerting of these questions focuses on the integrity of the measures being proposed in the war against terror. How do we distinguish genuine and meaningful public security proposals from those based on convenience and illusion, and yet avoid the appearance of ingratitude or cynicism toward those who might just be doing their best to help in the great partnership?

The picture is by no means all gloom and despair for a free Internet. We have been encouraged by innumerable positive developments in many countries, but advocates and reformers still have much to do. Expertise and participation is essential to ensure that appropriate regimes of protection and minimalist regimes of invasion are established.

We hope this report will go some of the way to answering these questions and providing some support and encouragement to the many people throughout the world who fight for a free and unfettered Internet.

Simon Davies
Director
Privacy International

Karen Banks
Co-ordinator
GreenNet Educational Trust

Executive Summary

Silenced is an independent research initiative managed jointly by Privacy International and the GreenNet Educational Trust. The twelve-month project was undertaken through a collaboration of more than fifty experts and advocates throughout the world. The work was made possible by a grant from the Open Society Institute.

The Internet has evolved to become an increasingly important platform not just for economic development, but also as a support for advocates who wish to express their opinion freely and to work toward the development of democracy. The medium has provided opportunities for citizens to participate in forums, and to discuss and debate issues that concern them. Unlike other media where the information flow is unidirectional - from the government to the masses - the Internet allowed a multi-way communication process giving the chance for anybody to air their opinions and views on issues affecting them. The development of the Internet has lead to more horizontal and less vertical communication. Control and censorship has a substantial effect on the Internet because it undermines confidence and trust in the medium and inhibits crucial flows of data.

This study has found that censorship of the Internet is commonplace in most regions of the world. It is clear that in most countries over the past two years there has been an acceleration of efforts to either close down or inhibit the Internet. In some countries, for example in China and Burma, the level of control is such that the Internet has relatively little value as a medium for organised free speech, and its used could well create additional dangers at a personal level for activists.

The September 11, 2001 attacks have given numerous governments the opportunity to promulgate restrictive policies that their citizens had previously opposed. There has been an acceleration of legal authority for additional snooping of all kinds, particularly involving the Internet, from increased email monitoring to the retention of Web logs and communications data. Simultaneously, governments have become more secretive about their own activities, reducing information that was previously available and refusing to adhere to policies on freedom of information.

Governments of developing nations rely on Western countries to supply them with the necessary technologies of surveillance and control, such as digital wiretapping equipment, deciphering equipment, scanners, bugs, tracking equipment and computer intercept systems.

The transfer of surveillance technology from first to third world is now a lucrative sideline for the arms industry. Without the aid of this technology transfer, it is unlikely that non-democratic regimes could impose the current levels of control over Internet activity.

One of the most important trends in recent years is the growth of multinational corporate censors whose agendas are very different from those of governments. It is arguable that in the first decade of the 21st century, corporations will rival governments in threatening Internet freedoms. Some American cable companies seek to turn the Internet into a controlled distribution medium like TV and radio, and are putting in place the necessary technological changes to the Internet's infrastructure to do so. Aggressive protection of corporate intellectual property has result in substantial legal action against users, and a corresponding deterioration in trust across the Internet.

A wide variety of methods are used to restrict and/or regulate Internet access. These include: applying laws and licenses, content filtering, tapping and surveillance, pricing and taxation policies, telecommunication markets manipulation, hardware and software manipulation and self censorship

There are some positive developments within this survey. Countries have established protections, countries have enshrined protections, companies have fought for the rights of privacy of individuals, technologies have sustained the ability of dissident groups to speak freely and access content privately, differences in laws in countries has sheltered the speech of the oppressed. Technological developments are being implemented to protect a free Internet, but the knowledge gap between radical innovators and restrictive institutions appears to be closing.

Contents

Introduction

I

Censorship in the Context of the Internet

There is an often quoted aphorism about censorship of the Internet, originally attributed to Electronic Frontier Foundation co-founder John Gilmore: "The Internet perceives censorship as damage, and routes around it."

Yet governments and commercial organisations relentlessly try to impose censorship. Their achievements in this quest have moved in a short period of time from the remarkable to the ordinary, to such an extent that in 1998 veteran privacy advocate Simon Davies warned Austria's *Cultural Competence* conference "I used to believe the Internet offered limitless opportunities for free speech; now I believe it is becoming a smorgasbord of opportunities for authoritarian control".

As this report demonstrates, the Internet represents both perspectives contemporaneously. The authoritarian trend, operating at a regulatory and a technological level, has been evolving ever since the first months of the Internet, but the September 11, 2001 attacks gave a number of governments the opportunity to promulgate policies that their citizens had previously opposed. The upshot has been an increased amount of legal authority for additional snooping of all kinds, particularly involving the Internet, from increased email monitoring to the retention of Web logs and communications data. Simultaneously, governments have become more secretive about their own activities, reducing information that was previously available and refusing to adhere to policies on freedom of information. To understand these changes, however, it is important to understand their context. This introduction explains both the historical background of censorship on the Internet and the technological realities of trying to implement such policies.

One of the most important trends is the growth of multinational corporate censors whose agendas are very different from those of governments. It is arguable that in the first decade of the 21st century, corporations will rival governments in threatening Internet freedoms. Stanford law professor Lawrence Lessig has warned that American cable companies seek to turn the Internet into a controlled distribution medium like TV and radio, and are putting in place the necessary technological changes to the Internet's infrastructure to do so. Such a future seemed impossible to the early Net pioneers; but in its day another medium was hailed as a democratising medium with truly public access. We now know that medium as commercial radio.

The price of freedom on the Internet, as elsewhere, is constant vigilance.

II

Action and reaction

Like most aphorisms, Gilmore's isn't exactly correct, in that it anthropomorphises the Internet. It is not the collection of computers, connections, and software that perceives itself as damaged; it's the people who use it, among whom there are always sufficient numbers who are angry enough to attempt to create a bypass around control. The reason for this reaction is an important psychological principle about Net users: in a world in which you are almost wholly represented by the words (and images, video files, and sounds) you contribute, any attempt to limit what you say feels like being put in jail without a trial. This psychological reality is rarely understood by outsiders seeking to control the Internet, and they are frequently surprised at the comprehensive ferocity of the reactions such efforts generally provoke. How, the average civil servant may ask, can anyone object to banning child pornography, hate speech, bomb-making recipes, or the personal details of secret service personnel? The answer is that most Netizens fear that any censorship, once put in place, may be subject to what's known among software engineers as "function creep". They start by removing child pornography and gradually turn the Net into nothing but advertisements and government propaganda.

This is, of course, nothing new: newspapers, radio, and TV have fought against government censorship in their time. What makes the Net different is that every machine attached to it has low-level access to the infrastructure itself. Everyone can be a publisher, distributor, broadcaster, and software engineer. The upshot is that trying to censor the Internet has a great deal in common with Hercules' predecessors' attempts to behead the Hydra. Chop off one head - say, the centralised file-sharing system Napster - and before long you find yourself fighting dozens more, in this case in the form of the decentralised file-sharing network Gnutella. Software writers can work much faster than politicians. One reason that governments are generally so concerned about the Net is that their policies may be moot by the time they have been passed by the legislature. This reality of modern life undoubtedly contributed to the speed with which legislatures rammed through their policies after the September 11 attacks.

It would be a gross mistake to separate the Internet politically and socially from the wider world. It is also a gross mistake to believe that governments cannot regulate on-line activity. The Internet is indeed a curious, fascinating and unique technological communications infrastructure; it is also very much a social and political infrastructure, and becoming more so an economic infrastructure. As we develop policies that appear to focus on the Internet, arguably feasible or infeasible, the policies are increasingly affecting non-Internet activities; and similarly in the other direction. That is, policies on censorship of the Internet will necessarily affect non-Internet practices. We have already seen how new laws on surveillance on the Internet have also been used to expand surveillance generally. Cyberspace is not a separate place or domain; it is a key component of our legal, political, economic and social lives. It is indeed a battleground for policies on censorship and surveillance, as much as it is a techno-political pawn to the forces that wish to limit freedom.

III

History

Battles about what kind of material should be available on the Internet are as old as the Internet itself, even though it is common to assume otherwise. In the early days, governments were only rarely the issue, since the network was primarily used only by academics and researchers. Rather, the small group of engineers that built the Net found themselves in positions of control, and like any ethical group, debated the consequences - hotly, as one does online. As the Net's population grew, those same engineers found themselves challenged to justify and find technological ways to maintain their control, and in many cases they (willingly or unwillingly) gave up that control.

One of the best early examples was the creation of the *alt* hierarchy on the collection of worldwide bulletin boards known as *Usenet*. Created in 1979, Usenet does not require the Internet to propagate; in its earliest days news was exchanged by direct telephone connections between machines. By the mid 1980s, Usenet developed an organised and orderly process for creating new newsgroups that persists today. Then and now, those wishing to create a new discussion group in any hierarchy except alt need to post a proposed charter to a newsgroup designed for the purpose and to newsgroups close in subject to the one that is being proposed. Readers of those newsgroups and other interested parties vote on the proposal. If it wins enough votes the group is created. But in 1987 that process was hijacked when a group known as the "Backbone Cabal" (so called because they could control newsgroup propagation) refused to create the newsgroup rec.drugs, even though it had been voted in. John Gilmore, later to co-found the Electronic Frontier Foundation, DEC's Brian Reid (who wanted a group called rec.gourmand, not rec.food.recipes), and Amdahl's Gorden Moffett, stepped in and created the alt hierarchy to host these discussions. The fledgling hierarchy began with alt.gourmand and alt.drugs carried on the servers the three controlled. A year later soc.sex passed its vote but the Cabal refused to create that, too, Reid created alt.sex, and, he noted in a memo, alt.rock'n'roll because it was "artistically necessary". Now, the alt hierarchy consists of tens of thousands of newsgroups.

The story is a perfect illustration of Gilmore's aphorism. The law of truly large numbers means that there is always someone somewhere in the world who is motivated to fight efforts to control the Internet - whether those efforts are self-serving or well intentioned. Regardless of the motivation, low-level control efforts have generally failed, especially when it comes to keeping specific information off the Net. Famous examples include the Church of Scientology's mid-1990s campaign to keep its most secret documents offline. These efforts involved lawsuits as well as attempts to flood the central discussion groups with huge amounts of material to drown out criticism. The result was that Net critics created many mirror sites in a variety of countries. This pattern has been repeated in many other cases, both large and trivial.

IV

Philosophies

There are two fundamental philosophies regarding access to information, which can be summed up as (1) Everything that is not explicitly permitted is forbidden; and (2) Everything that is not explicitly forbidden is permitted. These are generally referred to respectively as whitelists and blacklists. Because Web sites come and go so quickly on the Internet, maintaining lists of either type is a full-time job. Both types are used at the national level. Australia, for example, has a law requiring ISPs to block access to certain types of material deemed harmful to minors, including pornography involving children, animals, or excessive violence, and information about crime, violence, and drug use (a blacklist). Conversely, Burma has come closest to trying to block the entire Internet. There, it is illegal to own a modem or fax machine without a licence, and it restricts Internet access to a mere 800 whitelisted international sites, plus a few dozen available on the country's internal network.

You could think of traditional TV/radio broadcasting as effectively a whitelist, since only the programmes on the list agreed by broadcasters and broadcast authorities are transmitted. You could think of the telephone network as a blacklist, since anyone can make a phone call on any subject at any time, but there are certain published conditions under which service to an individual or business may be withdrawn.

The conflict in philosophy between these two particular classes of organisation has interesting consequences for the Internet, since both types are of key importance in providing Net connections, particularly now that they compete with each other to provide broadband connections. As both these types of organisations play major roles in building the Internet's infrastructure, it's not surprising that there are policy clashes between them as each tries to recreate the Net in its own image. So the TV companies and other 'broadcast' organisations set up geographically restricted services, and the cable companies talk about "content-based routing" that would give preference to the material they own, while the telephone companies and ISPs generally try to get policies accepted that hold them liable for as little as possible of the material they transmit or host on their servers.

Deciding whether the Internet is regarded as a broadcast medium, a content-neutral medium, or as a carrier, among other options, is a challenge for any policy-development process. Liability regimes for companies vary based on the philosophical approach adopted by national governments. Notably, according to Algerian law, all ISPs must take responsibility for the content of sites hosted; Swiss law only places liability upon the ISP if the true author can not be identified; in Hungary free-web space service providers are not responsible for the content unless the ISP is aware that the sites infringe the law and don't act against it; and the current legal thinking in the United Kingdom is that ISPs are regarded more like 'secondary publishers', like bookstores and archives, rather than a common carrier. Regarding ISPs as a carrier removes the responsibility of control and monitoring from ISPs. Regarding ISPs as a broadcast medium or a secondary publisher, however, makes them responsible for the content going through their pipes. Sometimes ISPs, depending on their business model, take on the liability through the services provided; mostly, however, the liability is decided by law.

Another difficult issue is that of jurisdiction. Traditionally, jurisdiction of government laws and powers are limited to servers within its geographic borders. Moreover, traditionally sites would only have to be held accountable for the laws in place within the jurisdiction where they are physically located. Such traditional views of jurisdiction have been replaced by more legally and technologically problematic interpretations. Some countries consider a source of information to be within its jurisdiction if it can be accessed by nationals, regardless of the physical location of the server. Court decisions in France and Australia, for example, have considered U.S. websites to be under the jurisdiction of their courts, and thus to French and Australian laws. This places service providers around the world in a problematic legal situation, in which they have to comply with laws from a number of jurisdictions, on top of complying with their own national laws.

V

Strategies

There are three means through which it is possible to control the flow of information across the Internet: legal, technological, and practical. While censorship may be perceived technologically as 'damage', in accordance with Gilmore's statement, legal and practical measures continue to be put in place. Many solutions, in fact, involve a combination of these three means of control.

Legal attempts may include government legislation, corporate lawsuits, or contracts such as the terms and conditions imposed by Internet service providers (e.g. 'Acceptable Use policies') or the End-User Licence Agreements (EULAs) imposed on software users. The sources of these regulatory strategies are thus from both government and industry; but may be invoked by individuals as well in the form of defamation and libel suits.

Technological attempts may include re-engineering the Internet to restrict its use as a distribution medium to only large rights holders; filtering software that blocks all but authorised content or that blocks content in specific categories; or sealing off content to all but authorised users. The first sounds impossible, but Stanford law professor Lawrence Lessig believes American cable companies are re-shaping and re-developing the Internet and its protocols to make it a reality. The second is promoted or mandated for use by a number of governments and policies, sometimes in specific circumstances, including Afghanistan, Argentina, Australia, Denmark, Hungary, Saudi Arabia, and South Korea, and the United States, to name a few. The third is typically used by commercial sites interested in making money from subscribers through restricting access to resources and

content, but a secure infrastructure with digital rights management can of course be imposed by anyone.

Practical types of control tend to rely on current limitations, so that the technology required for distribution is either unavailable or unaffordable for most people. In a number of countries reviewed in this survey, the cost of access is prohibitively high, allowing access to only the national elite. Market structure contributes to this problem in some regimes, where government near-monopolies in countries like Bahrain, Burma, Belarus, Tunisia and Liberia serve the dual-purpose of limiting market access and ensuring government control. Somalia, lacking a recognised government, has no licensing regime to allow for ISPs. Even market diversity doesn't promise a problem-free regime, however. In Bangladesh, the government cut off the lines of sixty service providers, arguing that they did not get their licenses renewed; but the providers argued that the interruption of service was to force them to stop providing internet-telephony in order to preserve the state voice-telecommunications monopoly.

As with technological means, practical means of control are not limited to government. Industry too may impose control. A good example of this would be the downloading of video, which until very recently required so much bandwidth to distribute that it was impractical for ordinary users. Accordingly, movie and TV studios were fairly safe from unauthorised copying and distribution. This situation is starting to change, however, as more and more consumers get broadband connections, disk storage continues to drop in price, and more effective methods for compressing video have become widespread. By 2004, trading TV shows and movies online will become as commonplace as music files were by 2000; and the movie studios will as a result begin taking a more active interest in suppressing file-trading through legal, technological, and other practical means.

But as previously indicated, the Internet is not some mute object in this process. It is a technological, social, political, and economic infrastructure that may 'strike back' against these means of control. Three notable ways in which the Net strikes back, as a result, include technological, practical, and commercial means.

Technological means of resistance is mounted through the many hacks of digital rights management systems. In 1999, for example, 16-year-old Norwegian student Jon Johanssen wrote a piece of software called DeCSS, which cracks the copy protection in DVDs. The original reason was that there was no commercial DVD player that worked on Linux systems; DeCSS was the means through which he could play his legally purchased DVDs on his system. But a version of DeCSS for Windows appeared quickly, and now it is possible to extract the files from a DVD and turn them into more compact versions (known as DivX) that can be more readily copied across the Net and played on any machine.

Practical fight-backs include simply redistributing material that is supposed to be kept secret. A common example is the code keys required to run many pieces of commercial software and shareware. It is very easy to find a valid code for such software simply by searching on Google. Similarly, when the U.S. government briefly threatened in 1990 to criminalise the domestic use of strong encryption, those who wanted it to remain legal distributed the free encryption software "Pretty Good Privacy" (PGP) on the Net so that any attempt to pass such a law would be futile. It is also a matter of course that any material that is forced off a single server on the Net, such as unauthorised MP3s or the secret documents of the Church of Scientology typically is posted on dosens of mirror sites within a few days.

Commercial responses are generally based on the supposition that consumers do have power. When Intel announced that it would include a serial number in each Pentium III processor that would make it possible to identify the processor involved in creating or copying any file, consumers and businesses revolted and Intel backed down. In general, while rights holders fight to protect their products from unauthorised copying, electronics companies continue making MP3 music players and software companies openly advertise software that transforms DVDs into readily copiable files. Similarly, anonymising services offer users who subscribe the ability to view content that may be blocked where they live, or simply protect their privacy. As long as there are commercial interests on both sides of the battle over Net censorship, consumers have a chance and a choice. Currently, however, the trend, at least among large U.S. corporations, is to back rights holders; Microsoft, with its Next-Generation Secure Computing Initiative, envisions incorporating digital rights management into all standard hardware and software products.

The same pattern applies, of course, to material that is not so harmless. Hotlines in a number of countries, including Australia, the Netherlands, the UK, Ireland, and the Baltic region, allow the public to report material they stumble across that they think might be illegal, such as child pornography. The people running the hotlines, for example the UK's Internet Watch Foundation, assess the report and examine the referenced material. If they find it is illegal, they report it to the police and

issue an advisory to British ISPs to remove it from their servers. While there are many fears that the IWF and similar organisations will overstep these bounds and move into legal but "undesirable" material or begin policing copyright violations, the system has so far removed a relatively small amount of material. In Australia, the regulating authority, the Australian Broadcasting Authority has found that most of its time is spent reviewing overseas web sites over which it has no jurisdiction.

The type of authority that oversees the regulatory process varies from country to country. Some are government departments, others are regulators, and in some situations they are independent bodies. Government departments regulate Switserland (where the police have sent letters directly to ISPs to block racist content), Italy (National Security Committee and Ministry of Communications), Laos (a committee including a number of ministries that establishes rules for internet users), and Tunisia (Tunisian Internet Agency, which is part of the Telecommunications Ministry), and Liberia (where the government directly intervenes through threats and detention). Regulatory bodies are responsible for deciding appropriate content. In Australia the Australian Broadcasting Authority can issue take-down orders to ISPs in Australia). In India (Communications Commission of India) and South Korea (Information Communication Ethics Committee) the bodies can remove content without court orders, as is the situation in Hungary (National Radio and Television Council). Relatively separate bodies may still contain government members, and may be heavily influenced by government. Some countries with such a model include the UK's Internet Watch Foundation created at first to fend-off regulation. Hungary has a Content Providers' Association, with similar origins but which has become more problematic with proposals regarding anti-porn filters, the erasure of 'vulgar and aggressive expression' or anything against 'good taste' and has made recommendations regarding potential copyright offences. The challenge is that these authorities are all bound by geography.

It is arguable that despite the best efforts of these regulatory bodies, even when access to a particular Usenet posting or Web site is blocked, the content itself is still out there. One of the characteristics of the Internet is that information recycles in many ways. Information contained in a Usenet posting that has been deleted from a particular country's servers may be mirrored on multiple Web sites, retrieved through Google's database of Usenet archives, saved as a file on an individual PC and copied across person-to-person file-sharing networks (P2P), or reposted repeatedly in an IRC channel created for the purpose. It is for all intents and purposes impossible to remove anything completely from the Internet. Even if every government and regulatory authority agrees that a particular bit of content is illegal and should be removed, as long as the Internet is an open-access medium for distribution, all the hundreds of millions of individuals who use it would have to agree for it to completely disappear. It is for this reason that most efforts to censor the Internet focus on blocking access to material rather than trying to remove it.

This property of the Internet also relies upon social action. While the caching properties of search engines and other services on the Internet may keep information available for a period of time after they are removed by governments, companies, or individuals; individual, community, and non-governmental action is often required. When news arises of an attempt at censorship, these communities and individuals around the world choose to host mirrors of the content, in many situations creating many more copies than were previously available. However, this is not always an automatic process, and requires the action of interested individuals; not all causes have interested individuals available with the time and resources to dedicate to this task. There are many kinds of content that so far have not found passionate advocates willing to set aside the time, effort, and expensive to digitise them and make them available. Great stores of books, movies, and music that are out of print are lost when rights holders do not believe they are commercially viable enough to bother making available.

There are a number of ways that citizens of a country that selectively blocks Internet sites can manage to gain access to those sites, depending on the nature of the government blockade. For example, there are certain sites that act as "anonymizers". Essentially, when you log onto those sites they act as proxies, accessing the site on your behalf and displaying the results while protecting your identity and without triggering the government-mandated block. The anonymising sites themselves may be blocked, but so many are run by people who vigorously oppose censorship, their addresses may change regularly to defeat the block. The difficulty then is for people seeking the sites to find out where they are. In such cases, up-to-date information about their location may be spread via Usenet, IRC, email, and/or the Web. Once people know where to look, such things are easily found. For this reason, China, through its Golden Shield, has at times blocked the main search engines, and carefully monitors the Chinese language portals that help novices navigate the Web. It isn't always necessary to block or delete material in order to limit the public's access to it: just make it hard to find. This obscurity is aided by unlikely forces. A number of

regimes are assisted through the use of technology developed in the west; for example China's Golden Shield is sustained by western-developed software and hardware applications and services to monitor and block access to on-line sources.

These technologies and techniques of blocking and monitoring are developed through politics, for specific tasks, and are also limited by technical means. One problem is that any attempt to censor the Internet by blocking material that arises from a keyword search (as Web filtering software and even spam filters intended to block junk email) is a blunt instrument that is likely to take out unrelated material. AOL, for example, had to tell some British users to misspell the name of their home town, Scunthorpe, when the name fell afoul of its software's built-in censor because of a string of four letters in the town's name. Similarly, attempting to block sexual discussions using keywords such as "breast" also block support groups for patients with breast cancer. Commercial blocking software has been shown to have another, less mechanical problem, in that the publishers of the software have been shown to block critical articles and analyses of their software. The latest victims of this "blunt instrument" problem were British MPs, who in early 2003 found it impossible to conduct electronic discussions of the in-draft Sexual Offences Bill after Parliament introduced a new system to block pornographic junk email. Other filters have been found to represent the interests of their proponents, blocking sites that promote safe sex, abortion, and even human rights organisations; even though these sites do not fall afoul of the legislative regimes within which they are developed.

VI

Mechanics

Obviously any censorship that is imposed by law can be enforced in the courts. This section looks instead at the technological ways that blacklists and whitelists can be enforced. An arising factor is the link between censorship and surveillance. Free speech and anonymity are tightly linked legally; as a result attempts to reduce free speech and to censor access to expression and attempts to speak freely are linked tightly with the ability to monitor access and link individuals to problematic expression. Dangerous developments have occurred on both fronts.

"The Internet" is not a single entity. On the physical level, it is a giant collection of computer networks held together by cable, telephone, and other connections. On the level at which most users think about it, it is a network across which many applications run, just as your single computer can run word processor, spreadsheet, and database applications. In popular parlance, "Internet" is often used as if it were synonymous with the World Wide Web (or possibly, the Web and email), but many more publicly accessible applications run across it than that. In order to understand how censorship and monitoring of access on the Internet work, you must understand what these applications are and how they interact. These include: Usenet, Internet Relay Chat (IRC), File Transfer Protocol (FTP), Hyper-text-Transfer Protocol (HTTP), Peer-to-Peer file-sharing (P2P), and instant messaging. The first three of these pre-date the Web (which is merely HTTP across the Internet), and go back to the Internet's text-based days.

Any of these services may be monitored. ISPs can log a huge variety of information about their customers, from details of email sent and received to lists of the Web addresses they visit, Usenet newsgroups they subscribe to, and IRC networks they access. Email is monitored more often than it is openly censored; Burma sorts and reads all email before it's delivered (possible only as long as you have a small user base and they use it sparingly), and the UK has proposed data retention rules under its Anti-Terrorism, Crime, and Security Act 2001 that would keep logs of transactional header traffic data for undetermined amount of time; other countries such as Switzerland, France, Spain, and Belgium have similar laws, for the most part implemented after September 2001. Algeria proposed to record the names and addresses of customers and their access to websites, although this practice was suspended; the law remains, stating that service providers must 'take all necessary steps to ensure continuous monitoring' so as to block access to censored sites. Germany's surveillance oriented G-10 laws involve strong advice for ISPs to 'police' content of websites. The Ukraine, Russia, Hungary, and the United Kingdom require that service providers implement monitoring capabilities for access by law enforcement authorities for a number of purposes. India requires that individuals present IDs for cybercafes in the city of Mumbai. Tunisia goes a step further allowing managers to monitor cybercafes for subversive activity, with plainclothes police regularly collecting details of internet activities; and most recently created a 'cyber-police' force to locate "subversive" websites to be blocked, intercept e-mail or attempts to reach sites containing "political or critical" material, hunt for and neutralise "proxy" servers used to get round directly-blocked access to sites, and track down and arrest "over-active" Internet users - the cyber-dissidents.

Ordinary email can be read easily in its entirety by any of the system administrators through whose

systems it passes en route to its final destination. For this reason, the usual way to protect the contents of email from prying eyes is encryption, which may also be used to protect files and other material posted on the Internet but intended only for a small audience of authorised users. Because strong encryption provides such a powerful mask for content, law enforcement battled throughout the 1990s to keep its use restricted. While it is fair to say that governments have for the most part lost the battle because of the needs of e-commerce, which uses encryption to protect sensitive information such as customer details and credit card information in transit; however, the more war-like atmosphere since the September 11 attacks has revived the desire to restrict encryption. At the time of writing, an early draft of the U.S.'s draft Domestic Security Enhancement bill 2003 proposes to add five years in jail to the sentences of those who use encryption in the course of committing a felony. Belarus still bans the manufacturing, maintenance, and use of cryptography products without the permission of the KGB. France still has an awkward regime surrounding the use of unlicensed cryptography, and China's laws are still very restrictive.

The Web is probably the simplest of all these applications to censor, in that a Web site is usually created by an identifiable individual and hosted on a commercial service. The would-be censor therefore has many options: contact the hosting ISP and ask that the site be taken down; arrest or sue the originating individual; or add the Web site's address to the database of sites citizens (or, in the case of commercial blocking software, customers) are blocked from seeing. All these methods have been used. The one risk in the case of the first two of these options is that removing a controversial Web site can sometimes be taken up as a cause célèbre by the rest of the Net - as happened in the Scientology case - and citizens of countries outside the purview of the censor may put up sites mirroring the original content as a protest. In the Scientology case, because the Church of Scientology is international and took up actions against individuals in many countries, critics created a rather clever site that contained none of the CoS's secret documents but allowed you to search the Net for their location on that particular day. The site of the secret documents' publication therefore became a moving target. In the third case, blocking technology, the risk is that users will figure out a way around it, such as by using anonymising (proxy) Web sites or accessing the content via other effective proxies such as the "cache" option on the search engine Google. Both function by acting as an intermediary, receiving the Web site themselves and displaying it for you, the virtual world equivalent of sending an unknown assistant to a bookstore to buy you a copy of a book you were banned from reading.

Blocking selected Web sites may be carried out at the national level, as in Bahrain, which blacklists sites such as the London-based Bahrain Freedom Movement, or Burma, which out of the entire Internet whitelists only about 800 sites in all. This may be conducted ideally in countries with limited numbers of ISPs, where access to the Internet does not follow from a decentralised model but rather goes through a government-run firm that is responsible for monitoring and blocking access. At the individual level, filtering software is available commercially across the Net and marketed in a number of countries both to parents worried their children will access undesirable material online and companies and other organisations concerned that their employees will abuse their work-supplied Internet connections by accessing pornography (which may have legal implications for the company). In the U.S., a law tying federal funding to the use of blocking software in libraries and schools is highly controversial. Blocking software typically relies on an internal database of undesirable sites, sometimes supplemented by specific words and/or phrases whose appearance on a site will cause it to be blocked. The commercial organisations that make this software are generally very secretive about the exact contents of these databases, although it is known that they often include sites above and beyond the classifications they say they block. In some countries, such as Denmark, South Korea, and Afghanistan schools, libraries, and cybercafes are required to use filtering software to protect the children who use their systems; such censorship falls disproportionately on disadvantaged people who must use these facilities for all their Internet access. The Swiss authorities have force the modification of DNS servers at ISPs to prevent access to a website about Swiss corruption. North Korea is probably learning from all of these methods: it is apparently working on developing an Internet for internal, though one with monitoring and control capabilities embedded by design.

Usenet news is a worldwide collection of tens of thousands of bulletin boards. The important characteristic is that these are asynchronous; people read news and post replies as they have time or when they're interested. Usenet newsgroups are organised by topic in a hierarchical structure that is meant to make it easy for individual computers and servers to subscribe to or refuse to carry specific groups or collections of related groups. Usenet pre-dates the Internet and does not need the Internet to propagate; news may be exchanged by computers directed connected to one another (for example by

phoning each other) using a bit of software known as Unix-to-Unix Copy Protocol (UUCP).

Like email, Usenet was devised to carry only text. In both cases, sending a "binary" file such as a picture, movie, audio file, or even a word processed document requires the sender to encode the file into text using one of a couple of commonly available bits of utility software (UUencode, MIME) and the receiver to decode them again into their original form (UUdecode, MIME). Most email users today are not aware of this intermediate step because it is handled seamlessly by their email software. It is considered rude to post binary files to most newsgroups, and there is an entire subhierarchy, alt.binaries.* just for the purpose. Besides the massive volume of discussions, therefore, Usenet is a significant medium for exchanging anything from old radio shows to pornography. Because binary files are much larger than text files, at times certain ISPs (and, controversially, for a time even some U.S. universities) have refused to carry the binary newsgroups when the amount of traffic became too great.

The only effective way to censor Usenet is to remove material from the servers that carry it, either by not carrying a newsgroup or hierarchy of newsgroups, or by removing specific material message by message. ISPs within a country can easily be directed not to carry specific newsgroups and can easily comply, which forms the basis of the hotlines mentioned above. However, it is perfectly possible for users to source a Usenet feed from a different service provider across the Net (for free or for a fee) and access the banned newsgroups that way. A number of such independent providers advertise a full and uncensored newsfeed.

Messages, once posted, can be cancelled either by the original poster or by a third party, but it is not foolproof as Usenet does not propagate consistently around the Net and a message that has already been downloaded by a user will remain on that user's hard drive, from where it may be reposted later. However, cancelling can be very effective even so. Although the cancellation message arrives at servers after the original message, it blocks the further distribution of that material. As far as is known, this is not, however, the method used by the hotlines set up in a number of European countries to allow the public to report illegal material (such as child pornography) found online. These, once they have examined the reported material and determined that it is illegal, report it to the police and direct ISPs within their countries to remove the material from their servers. In 2002, Britain's Internet Watch Foundation caused some concern by proposing to create a list of banned newsgroups that should not be carried at all by British ISPs, selected by criteria the IWF refused to make public.

Another case of Usenet in the United Kingdom involved a defamation case where an individual asked a service provider to remove offending posts. The service provider argued that their role was as more of a conduit of information; however the court decided that the role of the service provider was more that of a secondary publisher. As secondary publishers, according to British law are involved in 'processing, making copies of, distributing or selling' information, if deemed defamatory they are responsible for removing offending information.

The Usenet community does, however, support its own standards and operates its own system for removing unwanted junk, and this relies on the built-in ability to cancel messages mentioned above. The system began in 1994, shortly after the first spam began appearing. Essentially, volunteers with community endorsement issue "cancels" for messages that are posted to too many irrelevant newsgroups or too frequently to the same newsgroups. These days, the cancellation mechanisms are so effective that many newsgroups receive relatively little spam. Although there are some people who like to characterise these cancellation efforts as vigilante censorship, it's fair to note that: (1) Usenet spam drowns out legitimate conversation, arguably a bigger denial of free speech than cancellation; (2) the volunteers regularly publish information about what they've cancelled and what their cancellation criteria are (see the newsgroup news.admin.net-abuse for details); and (3) the standards for classifying a message as spam are not related to its content but rely on a mathematical index calculated from the range and number of newsgroups it's posted to and its general irrelevance to the actual topics of those groups. Most Usenet posters regard the cancellers as performing a valuable public service without which Usenet would be unusable.

IRC allows multiple users to exchange messages in a public or private setting in real time. At last count, there were approximately 450 public IRC networks (and an untold number of private ones). The largest of these networks typically supports about 130,000 connections at any one time. An IRC network is made up of hub servers (servers which simply direct traffic), and leaf servers (servers which hold users), all running a program known as an Internet Relay Chat Daemon (IRCD). Individuals wishing to access IRC need only download any one of dozens of free IRC clients. They may connect straight to an IRC server if they know the host address, or they may use one of

the servers the client software has in its internal list. Once connected, the user can see and type to others who have connected via any other server on the same network. So, for example, a user in London connecting to a server in the UK types a message to a user on a different server in the U.S. The message will pass from the first user to the UK server, be handed on to a hub server, which in turn relay it to the server in the U.S..

IRC networks are organised into channels that typically are named to reflect their topics of conversation. Many IRC networks have evolved sophisticated community standards and protections. For example, on the larger networks you may register your nickname and protect it with a password so that no one else can masquerade as you.

Each server has an administrator (usually someone affiliated with the server's sponsor), who has remote access to the server; each also has a number of operators. These volunteers keep the servers connected to each other on a day-to-day basis, as well as helping users recover passwords for their nicknames, ensuring channels run smoothly, and so on.

On most networks, anyone may create a new channel at any time and control who may access it. Accordingly, IRC is very difficult to censor entirely, since once two people have agreed on a network, they can create a private, invisible channel. IRC also has a function that allows two users who meet in a channel to swap files. Known as Direct Client-to-Client (DCC), this function transfers files directly between computers, and is used for anything from unauthorised copies of TV shows to work in progress to sharing child pornography. Because of the somewhat anonymous nature of IRC, accepting and running these files can be risky - a particular type of virus known as a Trojan is sometimes spread this way to infect the receiving computer with malicious software that turns it into a source for what are known as a distributed denial of service attack (DDOS). Because of these factors, because few journalists have ever used IRC, and also because of its minority, hobbyist nature, IRC is often portrayed in the media as a shadowy underworld inhabited only by paedophiles and thieves. The technology itself has legitimate business uses, as it provides a very cheap way to conduct conferences - discussions can be easily logged, and unlike telephone conferencing, it's easy to see who said what.

Censoring IRC is extremely difficult. Server administrators can certainly close down a specific channel or channels, but it's extremely unlikely they will do this. More commonly, the channels are managed by their "ops" - that is, operators, the people who created the channel. They may, for example, suspend or remove anyone at any time who abuses the channel (by for example flooding the channel with junk messages). Anyone who wants to run an IRC network where certain topics of conversation and types of behaviour are not tolerated will find it relatively easy to do so. What's difficult is convincing people to use that network instead of the others. For an outsider to censor a public IRC network is much harder. Server administrators, like the employees at ISPs, have little control over what users do on their networks. Channel operators, who do have some control in that they can kick people off for inappropriate behaviour, may be difficult to identify, as may individual users. Law enforcement wishing to catch active paedophiles are most likely to do so by either lurking in channels and logging the conversations or presenting the right sort of target to attract unsavoury attention by actively masquerading as a young teen. IRC's biggest protection against censorship is probably the relatively small size of its user base, and the fact that censoring a channel simply means the traffic will move elsewhere where it may be harder to monitor.

Other types of chatrooms, such as those provided by America On-Line's (AOL) proprietary client software and the ones provided on many Web sites, may work differently. On AOL, for example, there are volunteers who patrol many of the public chatrooms and may remove people for using language that falls afoul of AOL's Terms of Service (AOLers call this being "TOSsed"). Web-based chatrooms may either have human moderators or Terms and Conditions that allow them to terminate access for anyone who attracts enough complaints by other users. These Terms of Service are sometimes problematic, however, and may end up being corporate controls that force individuals to yield their otherwise constitutional rights to free expression. These terms of service end up acting as media-law, as argued within a study by Sandra Braman and Stephanie Lynch, two professors then at the University of Alabama.

The late 1990s saw the growth of peer-to-peer file-sharing networks (P2P), and these have been the target of many censorship efforts, primarily by corporate rights holders who believe (often correctly) that the content to which they control the rights is being traded by users. The first such service was Napster. Set up in 1999, Napster was a centralised file-sharing service that made it simple for users connected to one of its servers to search selected directories on the hard drives of all the other users connected to that server. Sued by the Recording Industry Association of America, Napster was ordered by the U.S. courts to block

the transmission of all material copyrighted by RIAA members. Since this was more or less impossible, the service was effectively shut down.

But Napster's capabilities were limited in any case by the requirement for a central server and the fact that users had to be connected to the same server in order to be able to share files. The next generation of incarnations of P2P, Gnutella and the many other services such as KaZaA, Morpheus, and eDonkey that sprung up in Napster's wake, operates as genuinely decentralised networks. Users connecting to Gnutella, for example, are able to send out a search request that combs the entire network of connected users. The RIAA has vowed to go after individuals distributing files via these networks. Morpheus and KaZaA were relatively easy targets, since the software is developed and distributed by commercial companies. With Gnutella, which is a product of the open-source movement and the work of a few dozen volunteer developers, the matter is more difficult. It is, however, possible that the RIAA and its movie industry sibling, the Motion Picture Association of America, may be able to identify heavy file-traders by noting the numbered Internet addresses of those offering large numbers of files using the "browse" feature in the software used to access the network. From there, prosecuting those users is a matter of getting the ISP that owns that numbered address to supply the name and address of the user assigned that number at that time. At the time of writing, a case is currently in the U.S. courts where a service provider is appealing to refuse the disclosure to the record industry of a subscriber's personal details in the interest of protection of privacy.

As things currently stand, legal scare tactics may be the only effective way of censoring a decentralised P2P network like Gnutella, built on free software, unless the Internet's actual infrastructure is changed to make the Gnutella network itself technologically impossible. There are, to be sure, initiatives to embed copy protection into audio and video files using digital rights management (DRM) software. These would not block the transmission of files over the network itself, merely ensure the files themselves could not be copied and successfully played.

So far almost all such systems have been successfully defeated by technological experts, although those creating DRM cracks or explaining how they work may be subject to prosecuting under 1998's Digital Millennium Copyright Act (DMCA), often even if they're not in the U.S. In 2001, for example, Dmitry Sklyarov, who wrote software by-passing the copyright protection in Adobe eBooks, was arrested at a hacker convention in Las Vegas where he'd given a talk about his work. In the end, he was not personally prosecuted, although Elcomsoft, the Moscow company for which he worked, was. The jury acquitted Elcomsoft, in part because writing the software was not illegal in Russia. In another case, when a 16-year-old Norwegian student named Jon Johansson wrote the software DeCSS to by-pass the system that protects commercial DVDs, he was subjected to charges by the MPAA press charges under the DMCA. The MPAA did not stop there, however: it also sued anyone who only linked to the software, including Eric Corley, the editor of 2600: the Hacker Quarterly, who (along with many others around the Web) linked to DeCSS from the magazine's Web site. Corley and 2600 lost in court and decided not to appeal.

VII

Conclusions: Present and Future Trends

The country reports presented in the next section of this survey show the richness of policies in the world. The world is not heading necessarily to a convergence on the destruction of free expression; but nor is the Internet necessarily the great liberator and source of resistance to censorship as presumed previously. The form and nature of censorship on the Internet has taken some surprising turns over the years, and these may be of use to future action by individuals and organisations who wish to prepare for, or cultivate national discourse on existing and future policies.

Regulatory Convergence

The technological mechanisms for censorship and monitoring of on-line activities have much in common, but they also face challenges because of the technologies involved. The use of filtering technologies preventing access to speech, take-down orders of speech, and surveillance techniques such as ID-checks and data collection are common across borders. However, the risks posed by these techniques and technologies provide similar challenges to an open society. Within any reasonable democracy, filtering technologies are not ideal from either the political or the technological perspectives; these weaknesses may be seized upon by advocates and activists to either force a change in laws through process or provide alternative techniques for preserving speech.

International agreements in this domain may prove to be troublesome to the cause of free speech. The work of the Council of Europe on its protocol to the Convention on Cybercrime attempts to harmonise laws on offensive speech of a xenophobic nature, giving both open and closed governments the mandate to introduce new laws. The surveillance procedures developed

within the Convention itself, as well as the work of the G8, sponsored by some of the most legally privacy invasive countries, and the possibly ominous developments of the World Summit on the Information Society, may converge leaving it possible to perceive the situation for free speech on the Internet as dire. It need not be so dire, however, so long as activists and advocates pay attention to these developments and inform themselves on programmes of action on both the domestic and international scenes.

The number of ways that speech is discriminated worldwide can only draw attention to the danger of restrictive regimes. Consider the multitude of ways that the term 'indecent' is interpreted by national laws. In Algeria, it is 'material that undermines public order and morale', and includes the 'denigration of the president through insults or defamation'. Similarly 'harming the honour and dignity' of the President is criminal in Kazakhstan. Argentina regulates in the name of 'respect for rights or reputation; protection of national security, public order, or public health or morals; for moral protection of childhood and adolescence; any propaganda for war and hate speech'. Australia regulates speech that is 'unsuitable for minors as well as child porn, bestiality, excessive violence, sex acts and information about crime, violence and drug use'. Bahrain blocks sites that are 'platforms for spreading biased news, rumours and lies; while Burma regulates any online writings 'detrimental to the interests of the Union of Myanmar and that are directly or indirectly detrimental to the current policies and secret security affairs of the government'. China uses the vague term of 'subversive' speech as the object of derision, and similarly to Burma, speech that 'advocates terrorism, threatens national security or national unity'. This is not far from the concerns of the Laotian government with its concern for speech that 'harms national unity'. Egypt warns against speech that discusses 'taboo issues, human rights violations, criticism of president, his family and the army, sex and modern versions of Islam; 'material with intent to corrupt public morals'; and 'putting old, false information' on-line. The Taliban perspective on speech is particularly illuminating of that regime, where speech was punishable if it involved 'vulgar, immoral, or anti-Islamic material'. Morocco also bans criticism of Islam, or of the monarch, or 'offensive reporting' by journalists. India regulates wherever speech is 'lascivious, or 'that appeals to the prurient interest'. Liberia blocked foreign sites that contain 'anti-Liberian material'; while Zimbabwe acts similarly for foreign sites that publish anything 'likely to cause alarm or despondency' or 'falsehoods'. Malaysia has used the coercive powers of the state to crack down on newspapers involved in speech that includes 'false accusations, could instil hatred towards government, contained seditious remarks that could create chaos in the country'; where *sedition* is defined as 'promoting feelings of ill-will and hostility between races or classes of the population'. South Korea, despite its high level of bandwidth use still regulates 'dangerous communications', and its regulator once barred 'offensive' information that includes 'porn, violence, hacking, euthanasia'; but this was deemed unconstitutional, where the 'offensive' was transformed into 'illegal' content. Spain reserves the right to shut down websites considered to have 'undermined' a list of social values; Turkey bans speech that insults state authorities. Other countries have gone to extreme lengths, surprisingly: in Switzerland, providing access to 'not allowed games' is illegal to combat betting on-line, while Greece has tried to ban some video games, as has a state in Australia. Tunisia goes so far as to require that ISPs sign a contract saying that they only allow customers use of the Internet for "scientific, technological and commercial purposes strictly to do with their area of activity", as it continual blocks the websites of opposition groups, NGOs, and foreign media. The above list is only a limited snapshot of the regimes of regulation in existence.

These articulations of 'offensive' and 'indecent' may again make the cause seem desperate. The power, however, of reminding democratic governments that their definition of offensive is alarmingly similar to that of China may give food for thought. Meanwhile, lessons learned from policy discourses in these western countries, and the technologies developed to circumvent laws as well, may give sufficient support to participation in other countries' policy discourses. Already Argentina modelled its national regime on the court decision in the U.S., *ACLU v. Reno* where the restrictive Communications Decency Act was struck down as unconstitutional. The best of all worlds can be brought forward to combat the worst cases, offering richer debates and discussions. Regardless, as long as a diversity of laws appears in the world, then speech can continue to exist through the spreading of censored expression in foreign jurisdictions; it is unlikely that all countries will harmonise laws to the fullest degree, allowing for some hope, and some opportunity to capitalise on jurisdictional arbitrage. Oppressed and opposition groups from a number of countries have seized on this opportunity.

There also remains hope as the market for provision of access and services remains rich. Countries with limited ISPs are more capable of centralising blocking services and controlling data flows across borders. North Korea is an ideal example here. The more ISPs and cybercafes,

however, the more complex regulation becomes with various ranges of market players, and larger lobbying forces, and more users with interests in the laws being created. Small and large ISPs alike are concerned with liability regimes within some laws, and may prove to be effective allies to advocates and activists in some policy discourses for the cause of minimisation of liability and protection of rights to free expression and privacy in the face of burdensome regulation.

This is not to say that the market is the ideal. In the U.S. where there are numerous players in the market vying for the attention of consumers we also see how the Terms of Services of providers actually limit the constitutional rights of users, permitting some speech and activity, while restricting speech and access that is otherwise legal. Attention must be paid to these developments as well, particularly as markets open up elsewhere.

Censorship beyond Governments: Industry

Most discussions of censorship tend to focus on governments as the agents. The concern regarding censorship and controls of data flows should instead be focused on where there are sources of control. Industry, particularly when it aligns with governments, can be a powerful source of censorship. In the name of copyright and intellectual property protection, alarming laws are passed and practices are accepted.

Some of these legal practices actually represent collisions of interests among industry. For example, Canada banned the provision of video streaming, iCravetv because it interfered with previous regimes on broadcasting. Denmark and Hungary have tenuous legal situations for the act of 'deep linking', where links to specific articles on news sites are made available instead forcing individuals to go through the front pages of these news sources. In the U.S. the content industry and the communications industry are in a legal conflict over the release of subscriber details of Peer-to-Peer services. In other situations, however, a collusion of interests arises. In contrast to the case in the U.S., Belgium has lead the way in 2000 with the tracking of users who use Peer-to-Peer applications, where ISPs provide names of their users to the music industry under a 'gentleman's agreement'.

Increasingly the world is following, dangerously, the U.S. in the realm of copyright. Europe is considering, for example, legislation analogous to the U.S.'s Digital Millennium Copyright Act (DMCA). So far, Denmark and Greece are the only European Union member states to introduce the necessary supporting legislation for the European Union Copyright Directive (the deadline was December 2002); the provisions are hotly debated elsewhere.

In addition, some end-user license agreements (EULAs) have attempted to limit what may be done with the software they accompany. For example, in 2002 the EULA accompanying video editing software produced by Ulead specified that the software could not be used to produce pornography. When challenged, however, the company agreed that the condition was vague, probably unenforceable, and inappropriate, and said it would remove the condition. However, the U.S.'s legal climate is likely to spur other companies to try imposing similar conditions.

Even if users were to 'tinker' with these applications, or with other applications make their means and applications made available they may face the wrath of the software industry, much as music-posters may face the wrath of the recording industry, with take-down requests as permitted by copyright law; as we saw with DeCSS. Again, though, not all courts of the world see matters similarly; Norwegian courts ruled that there was "no evidence" that the creators or users of DeCSS used the code; and so the creator of DeCSS was acquitted. The lessons from this case may be used in other courts and jurisdictions, even as laws are harmonised. Even as the laws are not harmonised, again jurisdictions may be used to the advantage of protection of speech; consider the decision in the Elcomsoft case in the U.S. following from the arrest of the Russian computer programmer Sklyarov. The court there decided that there was no 'willful' violation of the U.S. law, particularly as the alleged crime occurred in Russia.

Censorship beyond Governments: Libel and Defamation

Even individuals and groups, under the law, may also have the power to censor the conduct of others in the realm of libel and defamation. In a study in the United Kingdom, the Law Commission found that some ISPs received over a hundred complaints a year from solicitors and individuals regarding claims of defamation. The majority of the letters appeared to be from solicitors complaining about web sites created by disgruntled customers. Unfortunately, the Commission admitted that the safest course of action for the recipients of these letters of complaint is to remove the material 'without regard to the public interest or truthfulness', because of the legal status of ISPs under British law. The Commission worries that campaigning groups are most likely to be susceptible and subject to such letters; coming dangerously close to chilling political speech.

So long as ISPs are regarded as 'secondary publishers' or somehow responsible for the content hosted by their services, they are likely to be held liable. The Commission sees one possibility for countries is to exempt ISPs from liability completely, as in the U.S. Alternatively, clearer guidance is required as to the status of ISPs as publishers, archivists, or mere conduits and carriers. Moreover, additional attention must be given to the jurisdictional problems to libel and defamation, where a ISPs and content providers may be at risk from libel and defamation laws around the world, as we have seen in the case of Australia and the Dow Jones libel case where a U.S. website was considered under the jurisdiction of Australian courts. Even attempts by the EU to harmonise law have introduced new challenges and ambiguities that warrant further attention.

This situation, if not appropriately addressed, could lead to a situation where we have censorship by virtue of legal intimidation; either the intimidation of an ISP or the intimidation of an individual, chilling his right to speech. Censorship need not be written on the books of law; the mere fact that the books containing the laws may be perceived by the layman as an indication of fault and error may lead to censorship.

Implications

Intimidation is among the great threats to free expression; whether from the state, corporate interests, or fear of accusations of libel and defamation. Anonymous speech is a mechanism that protects individuals from intimidation; and this is what binds privacy and free expression tightly together, more tightly than the divisions that may exist. Lacking anonymous speech, and lacking anonymous access to speech, clear legal regimes must be maintained and respected to protect the right of the individual to speak freely.

In the context of the Internet, censorship only becomes more complex. With the introduction of new technologies; new voices with its potential liberalising role in making every individual a publisher; new laws from other jurisdictions with its potential to create a global village or metropolis; new means for expression with its potential to allow for code to enact our thoughts and wishes and aims; there are grounds for elation. The Internet does allow for expression, and does allow for some circumvention of traditional censorship powers.

The potential for increasing the powers of those who wish to control speech is equally alarming. Laws may reach across borders to threaten speech and action; copyright and libel concerns may chill speech before it is even spoken. Intimidation can emerge from many directions.

This is not a case of technology vs. the rest of the world. Rather it is a constant shifting of actors and interests, including technology. The world is rich in actors and systems of governance. Some of the conduct and speech is self regulated through norms and self-organisation, some of it is technologically regulated, some regulated by industry, some regulated by governments. Knowing these sources of regulation is the first step to finding ideal solutions to unjust attempts at control.

Therefore, it would wrong to say that with all of this damning evidence regarding the conduct of those with the potential to control, that all is lost. There are some very positive developments within this survey. Countries have established protections, countries have enshrined protections, companies have fought for the rights of privacy of individuals, technologies have sustained the ability of dissident groups to speak freely and access content privately, differences in laws in countries has sheltered the speech of the oppressed.

And advocates and activists still have much to do. Laws are needed, laws will be created; expertise and participation is essential to ensure that appropriate regimes of protection and minimalist regimes of invasion are established. Some would argue that laws are the anathema to free speech. Laws are needed to protect as much as they may cause harm. Without appropriate legal regimes, libel and defamation may place inappropriate burdens on ISPs; terms of service agreements developed within the marketplace may place a significant veil around constitutional rights; undemocratic sources of control may arise in even the most democratic countries.

The lack of laws may not be the ideal. In Mozambique the lack of laws regarding the Internet makes the press self-censor; surveillance is not enshrined in law in Senegal, opening the door to all types of abuses; in Kenya, the lack of Internet law allows the government to closely monitor on-line activity of the media. Laws can support and defend speech and privacy. What we are warning, however, is that once laws are created to restrict speech, then we must be aware of all the excuses used the world around to restrict speech; the mechanisms are the same, the techniques similar, and even the articulated intentions of 'offensive' and 'indecent' ring throughout. To sustain the powers of restriction privacy is invaded, rights are minimised, and surveillance increased in parallel with intimidation. The dangers are clear.

Activists and advocates, journalists and entrepreneurs, and the unstable balance of interests of all of the actors have so far created this

situation. Much remains to be done. Policies are yet to be formed; policies need to be questioned; laws repealed, destroyed, and built up again. Active individuals and a vibrant civil society are key to the goals and the results of our current action.

References

Cultural Competence conference. Linz, Austria, October 1998
http://competence.netbase.org/

Analysis of blocking software
http://www.peacefire.org

Historical development of commercial radio/ TV (covered by academic scholar Robert McChesney)
http://www.robertmcchesney.com

Historical context of Internet censorship: Wendy M. Grossman, net.wars and From Anarchy to Power: the Net Comes of Age (NYU Press 1998 and 2001). The full text of net.wars is online at
http://www.nyupress.org/netwars

Lawrence Lessig on threats of Intellectual Property, Future of Ideas, Random House, 2001.

Advantage ISP: Terms of Service as Media Law - - A Comparative Study Sandra Braman, University of Alabama, and Stephanie Lynch, University of Alabama, presented at TPRC 2002. Available at
http://intel.si.umich.edu/tprc/papers/2002/78/ AdvantageISP.zip

Law Commission report on Defamation and the Internet: A Preliminary Investigation, Scoping Study no.2, London, December 2002. Available at
http://www.lawcom.gov.uk/files/defamation2.pdf

Foundation for Information Policy Research, Implementing the EU Copyright Directive, Report, UK 2003
http://www.fipr.org/press/030908eucd.html

Internet Censorship in Africa
Regional report

In recent years, two major trends have become evident in the evolution of African communications and media legislation. On the one hand, there is the trend to address issues relating to the global digital divide which has led to the development of ICT policies that frequently identified the importance for African economic development of freedom of expression in the new media. Conversely, a number of African countries have introduced legislation, especially legislation directed at terrorism, that curbs a number of freedoms and that provides authorities with increased power to monitor and censor communications between individuals and groups.

> **"Some African countries use fear of harassment to keep the media in check in an effective campaign of self-censorship."**

Terrorism

The relationship between the fight against terrorism and the development of rights was encapsulated in the words of a Kenyan Minister during commentary on pending security legislation: "The Bill may be taking away a few fundamental rights of Kenyans and this may be justified by the very nature of terrorism, which is basically done in secret and by unknown people who do not advertise themselves".[1]

Throughout history, oppressive governments have used fear as a political weapon. The South African apartheid regime used the 'swart gevaar' (black danger) campaign to oppress a nation for over 40 years. By censoring opposition and by using its powerful propaganda machine, the government instilled a belief among white South Africans that every black man was a 'terrorist'. The current Zimbabwean government intimidates its citizens using fear of physical violence to prevent opposition to its rule. Some African countries use fear of harassment to keep the media in check in an effective campaign of self-censorship.

The US-led 'war against terror' has set the propaganda machine rolling with even greater vigor. Building on the fear generated from September 11's images of terror, 'cooperative' governments, such as South Africa, Kenya and Tanzania have been able to introduce repressive legislation in the guise of protecting the population from the 'evil' forces of terrorism (regardless of their respective stance on the war). Many other governments - having already given assurances that they will join the campaign - are following suit, with the result that national anti-terrorism laws that restrict freedom of expression may soon be widespread throughout Africa.

Anti-terrorism laws drafted after September 11 have in common the introduction of unprecedented powers for governments to intercept and monitor the communications of a wide range of organisations and individuals that oppose the actions and ideals of the ruling political authority. According to policy analyst, Gus Hosein, "Almost every country that changed its laws to reflect the environment following September 2001 increased the ability of law enforcement and national security agencies to perform interception of communications, and transformed the powers of search and seizure, and an increase in the type of data that can be accessed[2]."

South Africa's Anti-terrorism Bill (2003) is particularly interesting, especially since it has been widely criticised for re-introducing powers similar to those used in 1960 by the apartheid government to subdue liberation movements by declaring them 'terrorist' organisations. According to the Executive Director of the South African Freedom of Expression Institute, Jane Duncan, "South Africa is willingly walking into this terrain in a manner that confirms that it is with George Bush and against a host of now 'terrorist' national liberation movements, even those that ironically enough are following eerily similar political trajectories to that of the ruling African National Congress (ANC)[3]."

Increased surveillance powers introduced by the Regulation of Interception of Communications and Provision of Communication-Related Information Act (2003) compel service providers to indefinitely retain personal data that they have collected from customers, and make it available to law enforcement agencies when requested to. The act also makes illegal any communication service that cannot be monitored by the authorities, and gives the Minister of Communications broad powers to specify technical and security requirements, facilities and devices as well as specifying the type of communication-related data to be stored.

There are elements both of opportunism and lack of rigour in many of Africa's anti-terrorism laws. Kenya's latest anti-terrorism Bill contains a definition of terrorism that comes directly from the U.S. Patriot Act, South Africa's definition of terrorism has been taken virtually word for word from Canada's Anti-Terrorism Act (2001). Both definitions

are so vague that they could be used to declare virtually any opposition to government as 'terrorist' activity, resulting in brutal restrictions of the rights of those targeted to freely express themselves through any medium, especially the Internet.

In Kenya, the recently-published Suppression of Terrorism Bill[4] would make it a criminal offence to 'collect', 'make' (produce and make available on a website), or 'transmit' (by email, voice-mail or any other telecommunication method') any record of information of a kind likely to be useful to a person committing or preparing an act of terrorism (Suppression of Terrorism Bill, 2003: Part II, 5). This clause has sent local Internet users reeling in the midst of widespread controversy over a law that is likely to cause massive confusion as to which sites may be 'useful to terrorists'. The parliamentary committee charged with determining the legality of the legislation has opposed it, and hundreds of protestors recently took to the streets of Nairobi to voice their opposition to the Bill.

It will be interesting to scan the progress of the Bill, as the Kenyan government tries to appease the local population, while assuring the US and its allies that all attempts are being made to combat the type of terrorist attacks that the country witnessed in 1998 and 2002. The Bill followed on the heels of the lifting of crippling negative travel advisories and flight bans imposed respectively by the US and UK Compliance with the global campaign against terrorism is increasingly necessary to avoid the kind of costly sanctions imposed on poor countries such as Kenya, frequently criticized for not acting decisively against terrorist agents.

> **"Anti-terrorism laws drafted after September 11 have in common the introduction of unprecedented powers for governments to intercept and monitor the communications of a wide range of organisations and individuals."**

Corporate censorship

Another global campaign – the campaign to conquer the 'digital divide' – has created a profound effect on freedom of expression on the Internet in Africa. Firstly initiated by the at the 'Information Society and Development' Summit in 1996 in South Africa, followed by the G8 at the Kyushu-Okinawa Summit in July 2000[5] (though with a history dating back to some years before), the campaign aims to transform telecommunications as a key to economic development. The goals of the initiative are steadily filtering through to African governments as they prepare their countries' economies to welcome international investment in local ICT initiatives.

> **"National anti-terrorism laws that restrict freedom of expression may soon be widespread throughout Africa."**

The rise of ICTs and the convergence of old and new technologies has signaled a turning point in the telecommunications sector, where technologies such as Voice Over IP (VOIP) can now be used by Internet Service Providers (ISPs) to challenge telecommunications service providers' monopoly of voice traffic. Since most African governments are dependent on the revenue from their telecommunications monopolies, many have responded abruptly to attempts by ISPs to circumvent the national telephone network by raiding premises and sometimes even shutting off for long periods of time the country's access to the Internet.

Kenyan Internet activists, for example, reported that in September 2001, occasional raids on service providers together with the destruction of their equipment were common – particularly to combat illegal use of VSAT (Very Small Aperture Terminal[6]) in the country[7]. The monopoly provider, Telkom Kenya, would also block the country's access to the Internet for days at a time in an attempt to eliminate the use of VOIP (Voice Over Internet Protocol)[8].

Reform and liberalisation of the telecommunications sector is seen as necessary to increased accessibility of ICTs. Such reform is slowly taking place across the continent – but many governments remain wary about liberalising the telecommunications monopoly that generates some of its largest revenues. In many countries the crucial concept of competition and free markets has yet to be embraced even as a principle.

Because the telecommunications monopoly often controls local ISPs' access to the telecommunications network on which they

depend for the delivery of their services, the monopoly can effectively grant or deny access whenever it chooses. Some monopolies in Africa have used price increases to inhibit the growth of ISPs, others have simply cut off ISPs' access to the telecommunications network. All this has a negative effect on the consumer, who is often in effect censored from using the Internet as a tool for communication and expression.

In Zimbabwe, local ISPs contribute towards the harsh censorship being imposed on those in opposition to the government by refusing to host "political" websites[9] such as those of the Movement for Democratic Change (MDC) and the Zimbabwe Human Rights NGO Forum. These organisations have been forced to host their sites outside of the country, where they are subject to the policies and laws of countries that may not be sensitive to the urgency of their campaigns. The MDC's website, for example, has been shut down on two occasions for alleged spam abuse.

> **"If one lives in a society where one cannot speak out for fear of abuse, where journalists are being harassed, intimidated, imprisoned and even killed on a daily basis, then there is little hope of ending the culture of self-censorship that has pervaded many African countries."**

Laws concerning liability of web content have added to the problem of censorship of Internet content by ISPs'. In many countries, ISPs would rather remove immediately material considered potentially offensive, in case the content is later found to be illegal. It is essential that service providers are not given the responsibility for content held on their servers since most ISPs are driven by profit and not public interest. In April 1998, for example, the British transnational company, Biwater threatened the non-profit ISP, SANGONet in South Africa with legal action unless they immediately removed web content from the Mail and Guardian Newspaper archive website. The content was a newspaper article that contained allegations against the company that was the subject of a libel suit in the United Kingdom. It was linked to a news story that also covered the campaign against water privatisation in South Africa. Biwater's legal threat represented an attempt to censor information and discussion on an issue of great public importance in South Africa. On this occasion, SANGONeT refused to remove the content and the Association for Progressive Communications (APC) launched a global campaign to mirror the information in countries throughout the world. There are, however, many other cases where ISPs routinely remove content and consequently censor debate on the issue.

> **"In many countries the crucial concept of competition and free markets has yet to be embraced even as a principle."**

South Africa has since developed an e-commerce law[10] that limits the liability of ISPs to 'mere conduits' of Web content, and therefore limits liability for that content[11]. ISPs are, however, obliged to take down material if they are sent a 'take-down' notice from anyone who claims that the content or activity is unlawful. This leaves room for abuse when corporations, governments or individuals send notices in order to prevent public awareness or where they seek elimination of information that may question their authority.

Other African countries, for example Tunisia, have promulgated laws holding ISPs liable for content, including creating statutes requiring the ISP director to "maintain constant oversight of the content on the ISP's servers to insure that no information remains on the system that is contrary to public order and good morals"[12].

African Charter on Broadcasting

Initiatives that aim to drive forward the principles of freedom of expression have had a long history on the continent. The African Charter on Broadcasting, for example, sets out clearly-defined objectives for basing regulatory frameworks on 'respect for freedom of expression, diversity, and the free flow of information and ideas, as well as a three-tier system for broadcasting: public service, commercial and community'[13]. In terms of telecommunications and convergence, the Charter declares that 'The right to communicate includes access to telephones, email, Internet and other telecommunications systems, including through the promotion of community-controlled information communication technology centres'. Based on the recognition that Africans' economic, social and political development will

be dependent on access to ICTs, this particular aspect of the campaign has been debated at regional and international levels, for example at the World Summit on the Information Society.

The predominant theme that has emerged from these debates is that ICT and media policies should be developed in tandem. Lessons from the long struggle for freedom of expression should be taken into account when campaigning for a freer and more widely accessible Internet. ICT laws are often developed in isolation from media laws, with the result that ICT laws are developed from the perspective of a small, elite circle of ICT "experts", while media laws enjoy vibrant public debate aired on public media[14]. African civil society organisations and local media should thus be informed and engaged in ICT policy-making in order to carry through the protection of rights and freedoms to the new media.

"Perhaps the greatest force in censoring the views of Africans in the supposed "global information society" is the extreme poverty on the continent, made worse by global apartheid."

In a recent article on the 'right to communicate' campaign, John Barker and Peter Noorlander declare that the right to freedom of expression cannot be exercised in a hostile environment. This view recognises that at one level the growth in popularity of the Internet in Africa is dependent on the confidence that users have in the safety and privacy of the medium. If, for example, Internet users suspect that their online movements are monitored, they will exercise caution with regard to statements made or sites visited. Thus, 'the right to respect for private life must be guaranteed fully, including the right to communicate anonymously[15]'.

In assessing the vast number of ways that the Internet is, and could be, restricted as a medium for free expression in Africa, one begins to recognise the importance of considering the context in which such expression occurs. If one lives in a society where one cannot speak out for fear of abuse, where journalists are being harassed, intimidated, imprisoned and even killed on a daily basis, then there is little hope of ending the culture of self-censorship that has pervaded many African countries.

Finally, it is difficult to speak of Internet censorship in Africa without mentioning the salient fact that less than 0.01 percent[16] of Africa's population even has access to the Internet. Perhaps the greatest force in censoring the views of Africans in the supposed "global information society" is the extreme poverty on the continent, made worse by global apartheid. This was recently reiterated in a moving speech by the Africa caucus representatives at the July 2003 WSIS Intercessional meeting in Paris, France:

'We cannot see how a continent with limited capital, in monetary and capacity terms will attain equal opportunity for participation in an information society without a major shift in global economic imperatives and values'[17].

Thus, the solution to African Internet censorship lies as much in finding global solutions to these problems, as it is about reinforcing national and regional respect for freedom of expression on the medium of the Internet.

Footnotes

[1] Kenyan Justice and Constitutional Affairs assistant minister, Robinson Njeru Githae, http://allafrica.com/stories/200306300753.html

[2] Hosein, Gus, 'Beyond September 11, an excerpt from Privacy International and Electronic Privacy Information Center's Privacy and Human Rights 2003 report'

[3] 'Anti-Terrorism Bill will stamp on human rights' by Jane Duncan, http://fxi.org.za/antiterrorism.html, 10 January 2003

[4] Suppression of Terrorism Bill, Published in the Government Gazette on 3 July 2003

[5] The G8 Kyushu-Okinawa Summit in July 2000 was one of the first significant signs of commitment by wealthy nations to bridge the digital divide. It was at this event that the Digital Opportunities Task Force was initiated. The fourth point of the Okinawa Charter stated: 'We will exercise our leadership in advancing government efforts to foster an appropriate policy and regulatory environment to stimulate competition and innovation, ensure economic and financial stability, advance stakeholder collaboration to optimise global networks, fight abuses that undermine the integrity of the network, bridge the digital divide, invest in people, and promote global access and participation' (http://www.dotforce.org/reports/it1.html).

[6] VSAT is a secure and reliable medium to connect geographically dispersed locations. It is an earthbound station used in satellite communications of data, voice and video signals.

[7] 'The Internet: Triumphs and trials for journalism in Kenya' Okoth F. Mudhai and George Nyabuga, presented at Highway Africa conference in September 2001.

[8] See Kenya country report

9 'Internet censorship hasn't arrived in Zimbabwe (yet) but it's alive and kicking in the good old USA' Kubutana.net

[10] Electronic Communications and Transactions Act, 2002

[11] 73(1) A service provider is not liable for providing access to or for operating facilities for information systems or transmitting, routing or storage of data messages via an information system under its control (Electronic Communications and Transactions Act, 2002).

[12] The Internet in the Middle East and North Africa: Free Expression and Censorship, 1999, http://www.hrw.org/advocacy/internet/mena/liability.htm.

[13] African Charter on Broadcasting, Part 1.1, http://www.misanet.org

[14] See Ethiopia country report

[15] Towards a perspective on the Right to Communicate by John Barker and Peter Noorlander, FREEPRESS, April 2003 available on http://www.misa.org/freepress/FP%20April2003.pdf

[16] ITU Internet User Statistics, 2002

[17] African Caucus of the World Summit on the Information Society, July 2003

Cote d'Ivoire

Tucked into the western part of Africa, Cote d'Ivoire, with its 15 million population, has been hailed as the "heartbeat" of the West African economy. By the end of the 1980s, the one-party system gave way to the re-birth of democracy in the country. Human rights, including the freedom of expression, formed the cornerstone of the country's new dispensation. Cote d'Ivoire has, however, experienced an extended period of instability since a military coup d'état in 1999 followed in September 2002 by a large-scale military rebellion, both of which have divided the country.

The Cote d'Ivoire Constitution provides for freedom of expression, but in pactice this is restricted. Until recently journalists did not practice self-censorship and frequently criticized government policy, although members of the security forces continued to harass and sometimes beat journalists. The September 19 rebellion however, triggered a deterioration of press freedom and significant self-censorship from journalists did not wish to appear "unpatriotic".

Telecommunications has been an integral component of the government's developmental efforts. The Telecommunications Code was adopted in 1995 and modified in 1998. Also in 1995, the all-important *Agence de Telecommunications de la Cote d'Ivoire* (ATCI) was created as the telecommunications regulatory body.

The government has recognised the importance of the Internet, creating a ministry for ICTs in 2000. In mid-2002, there was an estimated 40,000 Internet users: 20,000 on dialup and another 20,000 on leased lines, but due to the war, at least one million people have moved out of the country, thus lowering the numbers further.

It is generally believed that the government in Cote d'Ivoire has been too concerned with access issues to censor information on the Internet. On one occasion, however, Aviso, the ISP belonging to the monopoly, Cote d'Ivoire Telecom, censored Internet phone calls to prevent threats to the monopoly by the use of Voice Over IP (VOIP). There was consequently a huge rise in telephone prices. The monopoly said this was due to telephone bills in rebel-controlled areas no longer being paid to CITelecom so that those in government-controlled areas now had to foot the bill.

With the civil war still raging in the country, the government is becoming more restrictive, ostensibly for "security reasons". The government recently called upon the website, www.abidjan.net regarding an article that was allegedly defamatory. They wanted the article removed and abidjan.net taken to court, but the owners of abidjan.net were found to be outside the country. A few of the more opposition-friendly newspapers in Cote d'Ivoire, that are also online, have received visits from military personnel for "security reasons", and have been harassed.

New trends are beginning to emerge in Cote d'Ivoire – especially since a cooperation agreement was signed between Côte d'Ivoire and the EU allowing telecoms companies to gain access to the SAT-3 satellite. Only when the war is over, however, will Cote d'Ivoire be able to build a free Internet. Until then, the fate of anyone who speaks out – against rebels or against the government – faces an uncertain future.

References

Agence de Telecommunications de la Cote d'Ivoire, (ATCI)
www.atci.ci

Aviso
www.aviso.ci

AfricaOnline
www.africaonline.co.ci

Globeaccess
www.globeaccess.net

AFNET
www.afnet.net

'Shooting the Messengers: Pauline Bax reports from Côte d'Ivoire for Index on Censorship' 15 November 2002
http://africa.oneworld.net

Egypt

Although the Internet has grown faster in Egypt than in other African countries, the government has attempted to control the development of the media. Threats of 'terrorism' and the protection of public morals have recently been used to explain attempts by government to limit freedom of expression on the Internet.

Recognising the benefits of Internet and ICTs for economic growth, the government has been very supportive of computer and Internet use and has made connectivity easier through a variety of universal access initiatives. The Egyptian government, through its Ministry of Telecommunications and Information (MCIT), seems committed to a goal of providing "a computer for every household".

Media in Egypt have been operating in a restrictive environment for a number of years – especially since the government enacted emergency powers in 1981. Until recently there were no restrictions on postings over the Internet or email, but in the last few years, especially after September 2001, the government has imposed numerous conditions on Internet freedom. The Internet is now monitored by the General Administration for Information and Documentation (GAID) which was formed in September 2002 by the Interior Ministry.

There has been a series of cases restricting content on the Internet. In October 2002, a Cairo appeals court upheld a one year jail sentence for violation of the law on distributing materials that corrupted public morals. Shohdy Surur had published a poem by his late father, the highly-regarded Egyptian poet Naguib Surur on a US based website and was forced to flee the country. Antiwar activist Ashraf Ibrahim has been detained since April 2003 for downloading information on human rights and from the al-Jazeera news site.

The government has also been using the Internet to impose conservative values. In 2001, for example, 52 homosexuals were tried by state security in 2001 after having been targeted through the Internet. According to Hossam Bahgat from the Egyptian Initiative for Personal Rights, the police have made 130 arrests for non-commercial, consensual, homosexual conduct since July 2001. "The police are engaged in active entrapment. There are officers whose only job is to fix meetings with men on the Internet, show up and then arrest them," he said. In February 2003, the appeal court upheld the conviction of Wissam Toufic Abyad for placing a personals ad on an Internet site and arranging through it to meet someone.

On 23 February 2003, the Egyptian parliament introduced a further extension of the country's state of emergency laws. According to the Egyptian Committee for the Defence of Democracy (CDD), the government's explanations that such laws are required to deal with 'terrorism' and 'drugs' are a disguise for the repression of the anti-emergency-state movement.

The laws, which are meant only for cases applying to terrorism and drugs, relate to a long list of crimes that have to be referred to state security emergency prosecution, established according to emergency laws. The list includes: 'calling by word of mouth or by writing or by any other means for the impediment of any provision of the constitution or laws; possession of written material that calls for or favours the previous actions; deliberate dissemination of news, statements, faulty or ill-motivated rumours or agitating news if the objective thereof is to disturb public order, induce fear in people, or causing harm to public interest or possession or development of publications that contain any of the previous crimes' (http://www.eohr.org/PRESS/2003/3-9.HTM).

In December 2002, the Egyptian Parliament adopted a new Communications Law. The Egyptian Initiative for Personal Rights (EIPR) was particularly concerned with Article 65 of the bill. As first presented, the clause would have expanded the government's power to engage in surveillance of private conversations and communications. The proposed text of the article allowed the Military Forces, Ministry of the Interior and the National Security Authority to access any communications network "in fulfilment of national security needs". The People's Assembly approved an amendment on 30 December 2002 and the article now starts by referring to citizens' legal right to protection of private life - the only reference to privacy in the entire law. It also restricts the right of security agencies to interfere with private communications except "within the limits specified by law". Parliament's Speaker, Fathi Sorour also demanded that a paragraph be added to the session's records specifying the legal guarantees for secrecy of communications in the Code of Criminal Procedures. Under those guarantees, security agencies can only interfere with private communications after obtaining a causal judicial authorization for no longer than 30 days and only in the course of investigating a felony or a misdemeanour punishable by more than three months of imprisonment.

With regional tensions rising due to the ongoing conflict between Israel and the Palestinian Authority and the regime change in Iraq, the prospects of a more open Internet usage policy is slim. The Internet is certainly being promoted

in Egypt, but its usage is constantly being limited by the increasingly stringent international and domestic clampdown on "subversive" trends.

References

The APC's Africa Policy Monitor Project
http://africa.rights.apc.org/research_reports/egypt.pdf

International Telecommunications Union statistics report, 2001
http://www.itu.int/ITU-D/ict/statistics/

Battleground Web, Al-Ahram Weekly
http://weekly.ahram.org.eg/2002/608/eg7.htm

Democracy Egypt Home Page
http://www.democracy-egypt.org/indexe.htm

The Egyptian Organization for Human Rights
http://www.eohr.org/

Human Rights Watch Egypt
http://www.hrw.org/mideast/egypt.php

Ministry of Communications and Information Technology
http://www.mcit.gov.eg/

Mid East Times
www.mideasttimes

Ethiopia

Access to information, freedom of expression and rights to privacy are enshrined in the Ethiopian constitution. Every one has the right to hold opinions and has freedom of expression without interference. Freedom of the press and other media and freedom of artistic creativity is also guaranteed without prohibition or any form of censorship. There have, however, been notable disagreements and lively debates as to how these broad constitutional rights should be interpreted and implemented to meet the needs both of the independent media and government's interest in the creation of a "strong" and "responsible" press.

With only 7.42 Internet users per 10 000 inhabitants, Ethiopia has been struggling to keep up with global developments in ICTs. ICT and media policies have, however, been in the process of development and are currently in their final stages. The Press Law, expected to be enacted later this year, covers freedom of expression, rights and licensing issues to engage in press activities and access to information. Groups such as Article 19 described aspects of the bill as "onerous" and called for it to be withdrawn.

Similar work is underway on the ICT policy plan but, unlike the Press Law, which experienced a vibrant public debate aired on public media, the ICT policy process was developed by a few elites and discussed within the circle of ICT "experts". The government has recently launched an extensive project to roll out school computer networks to 550 districts aimed at increasing access to the Internet. Interestingly, there is limited information as to how the relevant content will reach the schools.

The division between media and ICT policy means that issues relevant to privacy, access to online information and security are not discussed in detail in either policy document. Following September 11th, Ethiopia did not make changes to its laws and regulations to online privacy and free speech. However, as one of the countries that gave international assurances that it would join the global fight against terrorism and as occasional user of the Internet to disseminate information, the Ethiopian Government is cognizant of cyber crimes and online privacy and free speech. Recently, the government with the support of the UK Department for International Development began an effort to develop a Freedom of Information Act.

Ethiopia has a sole Internet Service Provider known as Ethio Stream owned by the public telecommunications operator. The Ethiopian government's control over the service provider makes it easier to handle legal issues concerning online privacy and to implement, if desired, filtering methods such as rating systems. The ISP can provide information about its subscribers to the courts when required by law. Ethiopia has no a national criminal law relating to spam, libel or other online issues that can be used for tracking offenders but in order to protect the revenue stream of its parent company the service provider continues to clamp down on cyber cafés that offer Voice Over IP.

Individual users can set up free email accounts and remain anonymous without interference. There is no requirement for users to identify themselves and there is no logging of the activities of users. Moreover, there are no public cases where users have been prosecuted. Most of the online content from Ethiopia is being hosted by a private web content company called EthioLink and the local ISP. Both EthioLink and the incumbent service provider have not made public any information on monitoring of Internet usage, communications and the actions of users, or on data retention. The online content hosted at these sites usually consists of static, relatively benign information about institutions. Online newspapers such as *Addis Tribune* and the *Reporte*r publish their online versions generally after paper copies are read by the public.

Ethiopia has not enacted a digital copyright act; nor is copyright is used to limit free speech. A draft national ICT policy makes some provisions for copyright of online information, but there is a general lack of legislation that deals with digital copyright covering software and peer-to-peer networks. The incumbent service provider has recently begun to provide .com, .edu, .org, .net, .biz, .info, .net, and .name domain names. Guidelines on domain names are generally sensitive to trade mark and copyright laws. Applicants are required to present certificates from the national trade registry office to obtain their domain names.

A close analysis shows that the monopoly of Internet service provision and cultural context of Ethiopia have contributed to a fairly stable Internet environment, with no known major security breaches thus far. The incumbent ISP has not used its customer information for commercial purposes, other than to announce its services. Cryptographic tools and products may be used at the discretion of users. The ISP has not so far been required to institute surveillance and wiretapping capabilities and there have been no public cases of leaks of Internet user information.

The ICT policy framework and action plan under development is expected to outline electronic freedom of information and access

to online government records. Government's commitment to enhance efficiency, effectiveness and transparency in civil service, its initiatives to enhance access to the Internet, particularly in the fields of business and education, and its efforts to create favourable policies for entry of the private sector to the Internet service market could lead to increase Internet usage. This in turn will facilitate the development of good online privacy and appropriate security policies to meet the challenges of globalisation and information age.

References

ITU Information Technology Statistics, 2002
http://www.ethiopianreporter.com/amh_newspaper/htm/important%20court%20cases/Preas2.htm

http://www.telecom.net.et/~estc/ICTPolicy/index.htm

Fostering the Capacities of the Ethiopia Civil Society to Influence ICT Policies' by Lishan Adam, APC
http://africa.rights.apc.org/research_reports/ethiopia civil society.pdf

Article 19, The Legal Framework for Freedom of Expression in Ethiopia, February 2003
http://www.article19.org/docimages/1513.doc
Internet from the Horn of Africa: Ethiopia Case Study', ITU, May 2002

Kenya

Kenya has one of the largest Internet sectors in Africa. Full Internet services were established in 1995 and the Communications Commission of Kenya (CCK) was recently formed to regulate the sector. It currently has over 30 licensed ISPs. The national operator, Telkom Kenya, has a monopoly for telecommunications services but plans for privatisation are in progress.

President Mwai Kibaki and the National Rainbow Coalition (NARC) recently won a landslide victory in the December 2002 elections with promises to fight corruption and to tackle Kenya's economic decline. Kibaki promised to end the autocratic rule of his predecessor, Daniel arap Moi, who had ruled Kenya for 24 years.

Before the NARC came into power at the end of 2002, there had been numerous cases of harassment, intimidation and imprisonment of media workers by state agents. This, together with legal restraints and commercial interference resulted in self-censorship among Kenyan media workers.

In May 2002, the Moi government passed a repressive media bill to effectively allow government to control the media ahead of the general elections that December. The Kenyan Media sector reeled with shock as the Statutes Law Bill (Miscellaneous Amendment Bill) was rushed through Parliament, forcing publishers to submit copies of their publication to the registrar before distribution and driving the cost of newspaper publishing bonds from 10,000 shillings (150 euros) to one million (15,000 euros).

Media observers were convinced that the Moi government used several indirect strategies, such as restricting bandwidth offered to ISPs through the state-owned Internet backbone, to censor Internet users in Kenya. In a 2001 report by Okoth F. Mudhai, media practitioner Lynne Muthoni Wanyeki was quoted as saying that the government sometimes demanded that ISPs produce their subscriber lists. In one case, she recalled an ISP that was forced to shut down a list created to discuss the 1997 general election out of fear about what was being expressed.

According to Internet activists, raids on telecommunications operators and destruction of their equipment were not unusual – particularly to combat illegal use of VSAT (Very Small Aperture Terminal[1]) in the country. The monopoly provider, Telkom Kenya, would often block the Internet in its attempts to eliminate the use of Voice Over IP (VOIP) which would compete with its telephone services. In December 2000 the Communications Commission of Kenya (CCK) ordered the closure of the month-old Kenya Internet Exchange Point (KIXP) ostensibly for infringing Telkom Kenya's monopoly rights.

The new government was voted into power on a platform of change and transparency. A few months into their governance, they have done away with restrictive licensing for broadcasting, VSAT operators are being licensed, the regulator is being reformed and a new telecommunications and ICT policy framework is being developed. In the recent June 2003 budget, duties on computers and accessories were removed and VAT was decreased across the board in a move to lower the costs of hardware for Kenyan consumers. However, in August 2003, Information and Tourism Minister Raphael Tuju announced the creation of a censorship board.

Terror attacks in Kenya in 1998 and 2002, compounded by the global anti-terrorism campaign has, however, initiated a new set of events that could prove a setback to the country's transition. Kenya's new anti-terrorism bill recently prompted an outcry by Muslims, the main opposition party, human rights lawyers and activists who say that the Suppression of Terrorism Bill, published in the Government Gazette on 3 July 2003, is 'repressive' and 'draconian'.

The bill would make it a criminal offence to 'collect', 'make' (produce and make available on a website), or 'transmit' (by email, voice-mail or any other telecommunication method') any record of information of a kind likely to be useful to a person committing or preparing an act of terrorism. This clause is followed by the statement that 'It is a defense for a person charged with an offence under this section to satisfy the court that he had a reasonable excuse for his action or possession' (Suppression of Terrorism Bill, 2003: Part II, 5).

Critics say that it will become extremely risky to use the Internet when users are unsure what constitutes information likely to be 'useful' to terrorists. Critics argue that other provisions of the bill relating to increased powers of search and seizure by the police, will lead to a growing sense of distrust and uncertainty in using the medium in Kenya.

The bill can be seen as a response by the Kenyan government to recent criticism by the UK and US that there have been too few arrests in connection with terrorist attacks in recent years. The Kenyan government wants to be seen to be acting decisively against terrorists in order to qualify for US aid – especially in the light of the crippling travel advisories and flight ban recently

imposed by countries such as the UK and US. The Administration of Justice and Legal Affairs Committee rejected the bill in July 2003, saying that it "threatens to tear apart the very fabric of one nation and could offer fertile ground for inter-religious animosity and suspicion".

Kenya has also recently launched a national review of its Constitution. According to Muriuki Mureithi, the draft Constitution recognises access to information as a fundamental human right and therefore views ICT policies and strategies as tools that not only provide access to communication, but aim to safeguard that communication. According to the draft Constitution, 'The Republic shall promote equitable development, recognise and enhance the role of science and technology, eliminate disparities in development between regions of the country and sectors of society, and manage national resources fairly and efficiently for the welfare of the people' (Kenya Draft Constitution, 14.15). Universal access to ICTs is consequently deemed a constitutional imperative not to be used for political expediency in Kenya.

References

International Telecommunications Union statistics report, 2001
http://www.itu.int/ITU-D/ict/statistics/

AISI-Connect National ICT Profile, Kenya
http://www2.sn.apc.org/africa/countdet.CFM?countries__ISO_Code=KE

Cybercrime: Kenya is a Sitting Duck
http://allafrica.com/stories/200109040536.html

Okoth F. Mudhai and George Nyabuga 'The Internet: Triumphs and trials for journalism in Kenya', Highway Africa 2001
http://www.highwayafrica.org.za/presentations/55.doc

Kenyans Must Reject Anti-Terrorism Bill, The Nation: 2 July 2003:
http://allafrica.com/stories/200307020986.html)

Constitution of Keyna Review Committee
http://www.kenyaconstitution.org/index.shtml

IFJ, East Africa Page
http://www.ifj-pa.org/docs/eastafrica.htm

Footnotes

[1] VSAT is a secure and reliable medium to connect geographically dispersed locations. It is an earthbound station used in satellite communications of data, voice and video signals.

Morocco

By all accounts, the Internet in Morocco is generally one of the most liberated in Africa, although access levels remain low due to the high cost for users. According to a Human Rights Watch report on Internet access in the region, "The government of Morocco does not restrict access to the Internet or censor content." This may be changing following the adoption of a new anti-terrorism law in June 2003 following the bombings in Casablanca.

Internet penetration is limited by the illiteracy rate (as high as 50 percent in the late 1990s), the cost of access, and the lack of access to computers and even phone lines (in the late 1990s, only 31.9 percent of Moroccans had telephone service).

Internet censorship appears to be limited. The US State Department reports that access to web sites run by the Islamist Justice and Charity Organization (JCO) are blocked. The Human Rights Watch report quotes Karl Stanzick, who manages a Rabat-based ISP called MTDS (Morocco Trade and Development Services), who said that no government approval is required to obtain an Internet account or post a web site, and "all Internet subscribers in Morocco can be completely anonymous if they wish." He added that the authorities have not imposed on ISPs any form of legal liability for materials they carry, and that he was unaware of any ISP that had been punished for "objectionable" content. Stanzick noted, however, that the "red lines" that inhibit political commentary in traditional media – the taboos on questioning the institution of the monarchy and Morocco's claim to the Western Sahara, and on "insulting" the King or Islam – also limit what Moroccans are willing to post in public chat-rooms and electronic bulletin boards.

The traditional media, however, are often censored by the authorities. Three journalists have been convicted under the new anti-terrorism law. Newspaper editions have been confiscated and top personnel fired for reporting on contentious issues such as the self-determination of Western Sahara or running interviews with for example the Polisario Front. Criticism of Islam or of the monarch is not allowed and many journalists have been censored for libel, national security violations or vaguely defined "offensive reporting". Newspapers use the Internet to publish articles that have been censored.

References

Agence Nationale de Réglementation des Télécommunications
http://www.anrt.net.ma/

Secrétariat d'Etat auprès du Premier Ministre, chargé de la Poste, des Technologies de l'Information et de la Communication
http://www.septi.gov.ma/

Morocco Internet Society
http://www.misoc.org.ma/

International Telecommunications Union statistics report, 2001
http://www.itu.int/ITU-D/ict/statistics/

Human Rights Watch: The Internet In The Mideast And North Africa - Country Profiles - Morocco
http://www.hrw.org/advocacy/internet/mena/morocco.htm

UNECA, NICI Infrastructure and Policy for Morocco
http://www.uneca.org/aisi/nici/Documents_English/moroccopub.en.doc

US State Department Country Reports on Human Rights Practices - 2002: Morocco. March 31, 2003
http://www.state.gov/g/drl/rls/hrrpt/2002/18284.htm

Mozambique

Mozambique's parliament adopted a new Constitution in 1990 that specifically guarantees the rights to freedom of expression and information and the right to independent print media. The 1991 Press Act developed and regulated these rights. It has since become common for citizens, institutions and the press to use the Press Law when demanding the right of reply or access to information. Mozambique is widely recognised as having one of the most free media in Africa.

Although growing rapidly, Internet usage is still largely confined to urban areas. In 1999 there were only 78,000 fixed telephone lines for a population of around 18 million, 70% of which live in rural areas. These figures have since grown to 242,100 for fixed line and 152,700 mobile subscribers based on 2001 figures. There is now Internet access from every provincial capital in Mozambique, and an embryonic network of telecentres in rural areas has boosted Internet user figures to 30,000 based on the ITU's 2001 statistics. There are 10 ISPs.

The government of Mozambique approved a National Informatics Policy at the end of 2000 and an Implementation Strategy in 2002. The policy specifically states that 'The State recognises and protects the right of citizens to have access to information and to knowledge spread by ICTs' and adopts the principal of universal access.

The policy and strategy also recognize the need for new legislation to cover specific needs related to ICT use. Constitutional rights have therefore been used to cover Internet use generically. Areas still to be covered by law include guarantees for the protection of personal data; data security and integrity for e-commerce; cybercrime; and the protection of intellectual property. The US State Department reports that oppostion parties reported their communications were monitored by the Government.

One area in the National Informatics Policy that could be considered a potential censorship threat as well as a defence of individual rights is a proposal in the policy to 'Combat the violation of citizens' rights and attempts against public order and social and cultural values, especially pornography, abuse and violence against women and children via the Internet'. The Constitution forbids incitement to racial or ethnic hatred in any form.

In current practice, there is no legislation curbing freedom of expression on the Internet, and no restrictions (blocking or filtering) on access to sites or the publication of information on the Internet. It has not, so far, been necessary to test the limits of the Constitutional precepts. Neither the government nor individual ISPs apply any form of censorship as far as it is known. Many independent newspapers have websites, and there is room on discussion forums and the like for criticism of both the government and political campaigning. There are no known cases of arrests or libel cases specifically related to material published on the Internet although the well known journalist Carlos Cardoso, who ran a fax-based newsletter Metical, was assassinated in 2000 by killers who were connected to the government. The newsletter was shut down by a libel suit by the son of the President in 2001. Two problems affecting the press are reflected to an extent in their Internet counterparts: self-censorship, and manipulation of information by external forces via the material corruption of journalists or editors.

With the growth of Internet use over the next few years some of these issues will undoubtedly have to be faced. It will be important to ensure proper debate of legislative proposals. Current trends indicate a fairly free environment for Internet use in Mozambique but the government's indications that it will join the global war against terrorism may see more restrictive laws being imposed in the future.

References

International Telecommunications Union statistics report, 2001
http://www.itu.int/ITU-D/ict/statistics/

Constitution of the Republic of Mozambique, 1990
www.kituochakatiba.co.ug/Mozambique.doc

Mozambique Information and Communication Technology Policy Implementation Strategy
http://www.infopol.gov.mz/pdf/strg_eng.pdf

Comissão para a Política de Informática
www.infopol.gov.mz
for National Informatics Policy and other documents

Mozambique home page
www.mozambique.mz

Instituto Nacional de Estatística
http://www.ine.gov.mz/
for national statistics
Statement by H.E. Mr. Carlos dos Santos Ambassador and Permanent Representative of the Republic of Mozambique to the United Nations on Measures to Eliminate International Terrorism. October 2001.
http://www.un.org/terrorism/statements/mozambiqueE.html

Mozambique, Country Reports on Human Rights Practices - 2002
Released by the Bureau of Democracy, Human Rights, and Labor, March 31, 2003.
http://www.state.gov/g/drl/rls/hrrpt/2002/18217.htm

Senegal

Senegal enjoys one of the most unrestricted media climates in the region. The constitution guarantees freedom of the news media and the independent media frequently criticize the government.

In terms of ICT development, Senegal is probably the leading Francophone sub-Saharan African country. The office for implementing the ICT component of the New Partnership for Africa's Development (NEPAD) is located in the capital, Dakar. The telecommunications sector in Senegal has recently undergone a complete restructuring as a result of the privatisation of the past national telecommunications operator. The new Telecommunications Act (December 2001) replaces the 1996 Telecommunications Act and institutes the Telecommunications Regulation Agency (Agence de Régulation des Télécommunications - ART) as the main player in formulating and supervising Senegalese ICT policies.

The Audiovisual Supreme Council (Haut Conseil de l'Audiovisuel - HCA) is an independent authority created in 1998 to control all audiovisual media. Internet content falls within the scope of the HCA but this body does not have a regulatory role. The functions of the HCA are to guarantee the independence and freedom of information and communication media; to ensure free and healthy competition in the sector; and to set rules relating to producing, programming and broadcasting that regulate audiovisual transmissions.

Before 2001, the national operator, Sonatel, played a pivotal role in the emergence of the ICT sector in Senegal by concurrently fulfilling access provision, regulatory, entrepreneurial and commercial functions. Since its privatisation and the creation of ART, a clear distinction has been established between public and regulatory functions, and private and operational functions.

Sonatel is divided into Sonatel Mobile and Sonatel Multimedia. The results announced in its latest annual report show Sonatel to be one of the most important enterprises in Senegal, with a degree of growth well above the national average. Sonatel is one of the leading economic powers, not only nationally, but also sub-regionally. The dominance of Sonatel in the telecommunications market in Senegal has received regular criticism from both the private sector and civil society organisations, who say that this dominance is an impediment to freedom of competition, lower access costs, and dialogue amongst all players in the sector.

Increasing awareness of privacy protection on the Internet is an emerging theme, especially in the Senegalese legal sector. Amnesty International Senegal is one of the leading organisations that emphasises the dangers of the current legal gaps to deal with issues such as encryption, protection of personal data, cyber crime and the possibility of recourse in the event of violation of privacy or security on the Internet. The Senegalese Telecommunications Regulation Agency plans to institute a free call service for users' complaints.

References

Participation of Senegalese civil society in the formulation of ICT policies by Marie-Hélène Mottin-Sylla, ENDA-SYNFEV
http://africa.rights.apc.org/research_reports/senegal_eng.pdf

International Telecommunications Union statistics report, 2001
http://www.itu.int/ITU-D/ict/statistics/

UNECA Senegal Country Profile
http://www.uneca.org/aisi/nici/Senegal/senegal.htm

The New Partnership for Africa's Development (NEPAD) Senegal
http://www.nepadsn.org

South Africa

In spite of efforts to introduce competition into the sector, South Africa still has only one fixed line provider for telecommunications services but will license a second one shortly. Internet growth was strong for several years but has slowed since 2001. The Constitution has some of the strongest protections of Freedom of Expression, right to information and privacy in the world. The government has enacted a number of controversial laws relating to communications in the last several years but Internet censorship has been limited to date.

South African Internet Service Providers are required to apply for Value Added Network Services licenses and to compete with each other in a monopoly market for fixed line services. (see above comment) Lack of competition in the provision of basic telecommunications services has contributed to a large void in the provision of services to the majority of South Africans. The provision of bandwidth is dominated by a handful of primary players of which the monopoly telecommunications provider, Telkom, holds a large slice. Since 8th May 2002 Sentech, the state-owned signal distributer has been licensed to compete and is supplying satellite bandwidth to the VANS and ISPs. It is assumed that Sentech will very shortly be a serious competitor in the data market.

Recent legislative changes aimed at bringing the South Africa legal system up to date with the present economic, social and political changes brought about by the information revolution have displayed a steep learning curve for both the market and the government. There are few Internet-specific laws. The Publications Act prohibits child pornography; bestiality and pornography that sexualizes extreme violence. It was amended in 1999 to cover Internet publications.

The first Internet law was the culmination of a number of years of consultation resulting in the Electronic Communications and Transactions Act of 2002. This Act provides the basic foundations for the legal recognition of electronic transactions and messages, and covers a variety of topics from defining computer crime to digital signatures and ISP liability, as well as providing measures for consumer protection and anti-SPAM measures. It also requires that encryption providers must register with the government.

There was considerable controversy over the provisions in the Act that transferred control over the .za domain from an industry run non-profit to a government appointed body. Subsequently, a Domain Name Authority that included critics of the ECT Act was created and nominations were announced for membership. The government received 108 nominations from the public and announced the choices in July 2003.

Another controversial provision gives the Minister of Communications the power to declare any database to be critical and to set standards for the administration of that database. Possible databases could include private medical databases, insurance records and even the .za zone file which administers the .za domain.

Perhaps the most worrying of these provisions involves the introduction of 'Cyber Inspectors'. Once introduced, these trained individuals will be given the power to aid law enforcement in criminal and civil investigations, as well as being granted the power to inspect and confiscate computers, determine whether individuals have met the relevant registration provisions as well as search the Internet for evidence of 'criminal actions'.

The Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002 has encountered a similarly controversial path. The Act, published in the Government Gazette on January 22, 2003 introduces new legislation compelling service providers to retain personal data that they have collected from customers for a period yet to be determined, and make it available to law enforcement upon request. It also makes any communication service which cannot be monitored by the authorities illegal, and gives the Minister of Communications broad powers to specify technical and security requirements, facilities and devices as well as the type of communication-related information to be stored.

A major opponent of this law, the South African Internet Service Providers Association (ISPA), stated that they were 'concerned about the personal privacy ramifications for our members, subscribers and customers. While the nature of law enforcement requires some encroachment into privacy rights, ISPA suggests that all data retention provisions be rigorously examined in light of the personal privacy guarantees contained in the Bill of Rights. While none of these rights are absolute in operation, ISPA believes that for the Internet to grow, citizens need to feel confident that their privacy online is given the maximum possible protection. Extensive data retention laws potentially threaten this vital confidence.'

Responding to the US's call for a global campaign against terrorism, South Africa has recently published the draft Anti-terrorism Bill (2003) which

seeks 'to provide for extended jurisdiction of the courts in relation to acts of terrorism (B12-2003). Some of the many critics of the bill decry the definition of terrorism that has been broadened to include any act 'likely to intimidate the public or a segment of the public', which critics have argued could be taken to include union strikes or demonstrations outside an embassy.

There is relatively active participation by the South African Internet society in the law-making process, bolstered by one of the most advanced constitutions in the world that guarantees the right to privacy and freedom from censorship. Internet-related news, especially in the areas of privacy, freedom of speech also receives widespread coverage in the country's media.

References

International Telecommunications Union statistics report, 2001
http://www.itu.int/ITU-D/ict/statistics/

Electronic Communications and Transactions Act (25-2002)
http://www.polity.org.za/pdf/ElectronicCommunications.pdf

ISPA final submission on the ECT Bill (8 May 2002)
http://www.ispa.org.za/downloads/ect/ispa_ect_sub_final.pdf

UniForum SA's Advisory to co.za registrants on the ECT Bill
http://co.za/ect/advisory.shtml

UniForum SA's submission to the Parliamentary Portfolio Committee on Communications.
http://co.za/UniForumECTBillSubmission.pdf

Bridges.org: South Africa's Electronic Communications and Transactions (ECT) Bill: analysis and commentary submitted to the Government on 6 May 2002
http://www.bridges.org/policy/sa/ect/index.html

ISOC-ZA's submission on the proposed ECT Bill
http://www.isoc.org.za/ectbill.htm

Comments on the Electronic Communications and Transactions Bill by Namespace ZA
http://www.namespace.org.za/020424A_ectresp.htm

Regulation of Interception of Communications and Provision of Communication-Related Information Act (A70 of 2002)
http://www.gov.za/acts/2002/a70-02/

ISPA Submission on Interception and Monitoring Bill B-20011 (August 2001)
http://www.ispa.org.za/downloads/PPC_8_aug2001.doc

ISPA Advisory 2: The surveillance of electronic communications:
Monitoring and interception laws in South Africa
http://www.ispa.org.za/advisory2.htm

Bridges.org: Interception and Monitoring Bill: analysis and commentary submitted to the Government on 14 August 2001
http://www.bridges.org/policy/sa/submissions/interception.html

Constitution of the Republic of South Africa (1996)
http://www.gov.za/constitution/1996/96cons.htm

South African ICT news daily
www.itweb.co.za

Tunisia

The Internet arrived in Tunisia in the mid 1990's and is now the most developed environment in Northern Africa. President Zein Al Abdeen Bin Aly has embraced the Internet in order to promote economic development.

Tunisia is considered the only Arab country that retains Internet technological independence, and has evolved its own Internet industry. Its creation of a high tech net medium ranked the country 51st position (out of 72 countries) in a UNDP league table of global technology achievements. The Tunisian government has a strong online presence. All Tunisian media have their own websites. Tunisian radio and television are broadcast live over the Internet.

The government has extensively invested in developing the telecommunication and telephone infrastructure and increasing the Internet bandwidth to assure more Internet penetration. It has allowed privatised companies to work both as ISPs as well as establishing cybercafes throughout the country. All universities and secondary schools are connected. Internet rates have been dropping, along with customs duties on imported computer equipment, making Internet access more affordable for Tunisians.

Although the government states that it advocates Internet technology, the State Security Police keeps the Internet under tight control, making sure that the usage conforms to the government's rules. The Internet regulations reflect the government's restrictive approach to freedom of expression and freedom of the press. In Tunisia, all news media, including the Internet, should promote the official line of the government and avoid news and commentary that imply criticism of government policies. The Agence Tunisienne d'Internet (ATI) works not only as the regulatory body for the Internet but also in the role of cyber-police as a watchdog over Internet usage and users. Like other media forms, Internet users perform self censorship in order to escape government restrictions.

The Tunisian government was an early adopter of Internet restrictions. In 1997, it enacted a decree that made ISPs responsible for their content and required them to submit monthly lists of their users. Encryption was also banned by a 1997 decree. A law on digital signatures was approved in 2000 and a new law on telecommunications was adopted in January 2001. The press code also applies to the Internet.

Several cyber activists have been arrested and questioned about their Internet activities and papers, NGO sites, and independent weblogs have been blocked. The editor of the Tunezine web site was sentenced in 2002 to two year imprisonment for criticising the government on his web site.

Tunisia is co-hosting the World Summit on Information Society (WSIS) in 2005. This has been controversial given the Tunisian governments actions against free speech on and off the Internet. A number of press groups and NGOs have called for the summit to be moved to a country more respectful of free speech.

References

Comite pour le Respect des Libertes et des Droits de l'Homme en Tunisie (CRLDHT)
http://www.maghreb-ddh.sgdg.org/crldht/index.html

Conseil National Pour Les Libertés en Tunisie
http://www.cnlt98.org/

Article XIX, Tunisia: Surveillance and Repression
http://www.article19.org/docimages/660.htm

Human Rights Watch on Tunisian Internet Censorship
http://www.hrw.org/advocacy/internet/mena/tunisia.htm

Tunezine
http://www.tunezine.com/

www.alternatives-citoyennes.sgdg.org

Agence Tunisienne d'Internet
http://www.ati.tn/

Arrêté du ministre des communications du 9 septembre 1997, fixant les conditions d'utilisation du cryptage dans l'exploitation des services à valeur ajoutée des télécommunications. http://www.infocom.tn/juridique/arrete9-9-97.htm

Arrêté du ministre des communications du 22 mars 1997 portant approbation du cahier des charges fixant les clauses particulières à la mise en œuvre et l'exploitation des services à valeur ajoutée des télécommunications de type Internet
http://www.infocom.tn/juridique/arrete22-3-97_internet.htm

Loi n°2000-83 relative aux échanges et commerce électroniques
http://www.infocom.tn/juridique/ecommerce.htm

Loi n° 1-2001 du 15 janvier 2001 portant promulgation du code des telecommunications
http://www.infocom.tn/juridique/code_telecom.html

Zimbabwe

Media in Zimbabwe operate in one of the most repressive environments on the continent. Media workers are regularly harassed, detained and beaten by the police, with the cumulative effect that self-censorship prevails in both the media and civil society in Zimbabwe. The Internet has generally escaped government censorship because of its relatively low user group, but restrictive media laws have been introduced that can be used against Internet communications.

One of the first such laws was the Posts and Telecommunications Act of 2000. This act maintains that if, in the opinion of the President, it is necessary in the interests of national security or the maintenance of law and order, s/he may give a directive that any class of communications transmitted by means of a cellular telecommunication or telecommunications service (including email) may be intercepted or monitored in a manner specified in the directive (Section 98 (2) (b)). It is unknown if this has been used yet but the US Statement Department in their 2002 Human Rights Report stated 'The law permits the Government to monitor and intercept e-mails entering and leaving the country, and security services reportedly have used this authority to monitor e-mail communication, although the extent of this monitoring was unknown."

Many laws that deal with issues of broadcasting and public order were enacted to limit freedom of expression of the media including the Broadcasting Services Act, the Zimbabwe Broadcasting Corporation Commercialisation Act and the Public Order and Security Act (POSA). POSA is particularly notorious as it makes it a criminal offence to publish anything "likely to cause alarm or despondency" (and carries a prison sentence of up to seven years). The government blocks certain sites using legislation such as POSA.

Another particularly dangerous law is the misnamed 2002 Access to Information and Protection of Privacy Act that requires reporters to be licensed. It has led to the arrest and detention of a number of journalists including Andrew Meldrum, a reporter for a British newspaper, The Guardian, accused of "publishing falsehoods," even though the newspaper is available solely on a UK Web site. The case was dismissed by a court but Meldrum was expelled from the country.

The website of the Movement for Democratic Change, www.mdczimbabwe.com, has been shut down a number of times by its US ISP, Valueweb, for supposed spam abuse. Activists in Zimbabwe claim that 'dirty cyber tactics are being used to destabilise the MDC's communications'. This has occurred at critical periods, for example just before the MDC's call for a nation-wide stay-away and more recently, just before US President, George Bush visited Africa and the African Union met in Maputo. The MDC was forced to have its site hosted by an external ISP when Zimbabwe Online (ZOL) declined to accept the MDC and Zimbabwe Human Rights NGO Forum as clients in anticipation of political pressure on local ISPs. The MDC's offices are regularly raided while intelligence agents view information stored in their computers.

Vibrant political discussion occurs via email and on Internet forums in Zimbabwe. The Chronicle (a state-controlled newspaper in Bulawayo) was recently hacked and information critical of Zanu PF was placed on its home page. Civil society organisations such as Kubatana.net have offered an alternative to the traditional media by providing a platform for stories that would in normal events be censored. Ordinary Zimbabweans have used Kubatana to publish their stories of illegal detention and torture; the media have sometimes used stories from Kubatana in their newspaper publications; and Zimbabwean civil society organisations have used the Kubatana directory to organise seminars, conferences and workshops.

References

International Telecommunications Union statistics report, 2001
http://www.itu.int/ITU-D/ict/statistics/

Media Institute of Southern Africa (MISA)
http://www.misanet.org/

MediaChannel.org, In depth: Zimbabwe Censorship
http://www.mediachannel.org/originals/zimbabwe.shtml

Zimbabwean Media in Crisis: Issues and Challenges, Sizani Weza
http://pcmlp.socleg.ox.ac.uk/transition/issue2_3/weza.htm

Enforcing the Rule of Law in Zimbabwe.
http://www.hrforumzim.com/special_hrru/Special_Report_3_Rule_of_law.rtf

Access to Information and Protection of Privacy Act (AIPPA)
http://www.kubatana.net/html/archive/legisl/030611aippaamd.asp?sector=LEGISL

Broadcasting Services Act, 2001
http://www.kubatana.net/html/archive/legisl/010404broa.asp?sector=LEGISL

Public Order and Security Act, 2002
http://www.kubatana.net/html/archive/legisl/020122posa.asp?sector=LEGISL

Geoff Feltoe, A Guide to Media Law in Zimbabwe, 2002
http://www.misa.org/legislation/Zimbabwe/Media%20Law%20Zimbabwe.pdf

Kubatana
http://www.kubatana.net

Internet censorship in Asia
Regional report

For a growing number of people in the Asian region, the Internet has become an important tool for communication and sharing of information and knowledge— Growth of access, particularly in urban centres has been strong and steady, but in many areas the technology to access the Internet is not yet available. At the same time, governments throughout the region are moving to impose various kinds of restrictions on both access and content, endangering the right to privacy and curtailing freedom of information and expression.

> **"Governments throughout the region are moving to impose various kinds of restrictions on both access and content, endangering the right to privacy and curtailing freedom of information and expression."**

Like the other regions, Asia has over the past decade experienced a revolution in information and communications technology. The phenomenal growth of the Internet in most countries in Asia has greatly facilitated information exchange and communication among people. Widespread Internet use in Asia is partially a result of the region's economic growth levels and consequent improvements in the quality of life of the population. With more people expected to go online due to higher incomes, better communication could lead to further economic growth and an end to poverty that still afflicts many parts of Asia.

Governments across Asia recognise the potential of the Internet for economic, political and social progress, and most of them encourage the development of the infrastructure that would make this possible. The proliferation of Internet service providers and the consistent growth in the number of Internet subscribers in many Asian countries indicate that the ICT revolution has taken hold substantially in Asia.

China's experience is worth noting. Since the mid-90s, Internet use has vastly expanded to an estimated 45 million people. While this number is small in comparison with the country's population of 1.3 billion, the Chinese have increasingly connected to the Internet as part of government efforts to propel China's economic growth.

India has also seen a rapid increase in Internet use recently. With 7 million Internet users out of a total population of 1.2 billion, the Indian government is crafting new regulations to further increase Internet access levels throughout the country.

South Korea, like China and India, recognises the pivotal role of the Internet in economic development. With more than 24 million Internet users, South Korea also has one of the world's largest concentrations of high-speed Internet connections.

The Philippines has 2 million Internet users, but they are mostly concentrated in the urban areas. Although households with personal computers account for less than three percent of the population, the country has a high density of mobile phone ownership, with an estimated 12 million subscribers sending out a huge volume of text messages daily.

Two of the most economically advanced countries in Asia-Pacific are also heavily wired to the Internet: Australia has between 5 and 6 million users and New Zealand, 1.5 million.

In contrast, Asian societies that have remained closed to the outside world have few Internet users. North Korea has no Internet service providers and only a handful of citizens are allowed to go online.

> **"While the technology has the potential to bring Asian countries closer together, the reality is that disparity in access has also created a digital divide in the region."**

The picture that emerges from this brief survey is that, like elsewhere in the world, the Internet has grown significantly in Asia. Yet, while the technology has the potential to bring Asian countries closer together, the reality is that disparity in access has also created a digital divide in the region. People living in the more affluent countries are in a better position to benefit from access to information on the Internet than those still trying to get a foot onto the economic ladder. Within societies, the more affluent sections living in the urban areas are more likely to access the

Internet than those in the rural areas, where the priority is to feed the hungry rather than get a dial tone. While economically advanced countries like China and South Korea are barreling down the information superhighway at top speed, less developed ones like Burma and North Korea have scarcely recognized the advantages.

Pulling the plug on free expression

Although most governments in Asia recognise the benefits of information and communications technology and do in fact acknowledge the important role of the Internet in the economic, political, social and cultural spheres, a number have over the past decade imposed tight restrictions on its use.

In the aftermath of 9/11, some governments in the region have invoked counter-terrorism initiatives to crack down on Internet content.

Indian authorities are implementing stricter surveillance and monitoring controls over Internet activities, especially after 9/11 and the December 13 attack on the Indian Parliament. The Prevention of Terrorism Ordinance authorises the government to monitor without legal restriction all kinds of electronic communications, including personal e-mail.

The Philippine Congress is presently considering an anti-terrorism bill that proposes sanction arrest and detention without court orders, the sequestering of bank deposits and assets of suspected terrorists and their supporters, and which authorises the government to conduct wiretaps on those even remotely suspected of involvement in terrorist activity. Human rights groups fear that the proposed law, that permits surveillance of the Internet and e-mail, is intended to intimidate critics of the government and could violate the constitutional guarantees of free speech and free expression.

The New Zealand government now has the legal authority to inspect computers and monitor private e-mail as part of a campaign against terrorism and crime. The Crimes Amendment Bill, introduced in November 2000, seeks to prohibit hacking and includes provisions on protecting online privacy. It also requires users to hand over encryption keys and allows the police and intelligence services to hack computers. It has been strongly criticised, however, by many quarters as lacking adequate safeguards against abuses.

Other Asian states cite national security as the primary reason for restricting Internet content. Targeted by some states are those who organise protest actions on behalf of groups or movements whose goals are deemed detrimental to state policies, the national interest, or even "public safety".

"In the aftermath of 9/11, some governments in the region have invoked counter-terrorism initiatives to crack down on Internet content."

The Chinese government has created perhaps the world's most blatant and elaborate system for Internet monitoring and censorship. On the one hand, China's official policy has been to widely promote access, so that people can actively take part in economic construction. On the other hand, the government has also begun to limit Internet usage by way of a combination of new technology and legal rules, as well as traditional techniques of surveillance, intimidation and arrest of critics. Despite these restrictions, people have used the Internet to expose cases of official corruption, negligence and wrongdoing, and to organise protest actions against state repression.

The South Korean government has also become active in censoring Internet content that it considers "dangerous" and "harmful" to national security. In 2002, the government closed down a website for two months that argued against compulsory military service for all Korean males. Later that year, police arrested a member of a political party for uploading materials related to North Korea on the party's website, claiming that doing so violated national security.

In Kazahkstan, the media and the Internet are tightly controlled by the President and his family. Existing laws allow the government to crack down on websites critical of its authority, and prohibits the release of information detrimental to the state. Web sites are required to be registered with the government.

Some countries have enacted legislation that would deter and punish those responsible for cybercrime, cyberfraud and the dissemination of computer viruses. These laws could have a chilling effect on legitimate advocacy on the Internet.

The Philippines has enacted laws to cover different types of cybercrime, including computer hacking, virus distribution, computer fraud, and computer forgery. In India, cybercafés and the homes of Internet users can be searched at any time without a warrant if cyber crime is suspected.

The Information Technology Act of 2000 contains provisions that will allow authorities to crack down on Internet content deemed objectionable.

> **"Countries have moved to impose strict limitations on access to the Internet because they fear that contact with the outside world by their citizens, particularly political dissidents, would erode their hold on power."**

In Australia, recent amendments to the Broadcasting Services Act spell out the types of material that can be banned from websites and newsgroup servers, including pornography involving children, bestiality, excessive violence, real sex acts and information about crime, violence and drug use. But online content censorship laws such as this have met with opposition from civil liberties groups which argue that this could have a significant effect on the legitimate use of the Internet and may affect the fair reporting of news and current affairs. The Cybercrime Act, approved in October 2001, gives magistrates the power to order Internet users to disclose their decryption keys.

South Korea has censored Internet sites it considers harmful - especially to young people. These include sites dealing with pornography, violence, computer hacking and the spread of viruses, cybercrime, and euthanasia. Later, the list was expanded to include gay and lesbian content.

A handful of countries have moved to impose strict limitations on access to the Internet because they fear that contact with the outside world by their citizens, particularly political dissidents, would erode their hold on power.

The official website of the North Korean government, not unexpectedly, toes the government propaganda line and ignores completely the dire realities of life under the repressive regime of Kim Jong-il. But groups such as the Citizens' Alliance for North Korean Human Rights, based in South Korea, are using the Internet to assist those who manage to escape from the country and to bring to light what is happening behind the Iron Curtain.

Since the mid-90s, the military regime in Burma has imposed very strict rules on Internet access. Anybody who uses the Internet to "undermine the state, law and order, national unity, national culture or the economy" faces a 15-year prison term. Anyone who creates a link to an unauthorised website also faces a prison sentence. Since January 2000, online political material has been banned and websites can only be set up with official permission.

Conclusion

Asia is characterised by a cultural diversity that allows societies to adopt practices unique to their value systems and historical experience. The right to privacy may be assiduously defended in the West, but it may well be an alien concept in parts of Asia where traditional kinship ties remain strong. Thus, governments justify moves to restrict Internet content by claiming that these are "harmful" or "dangerous" to society when what is considered "harmful" or "dangerous" in one country may be perfectly acceptable in another.

An important issue to consider is the extent to which states can regulate or limit Internet access or content without infringing on fundamental freedoms and basic rights guaranteed under the Universal Declaration of Human Rights.

China, for instance, insists that it has the right to clamp down on websites that are clearly anti-government. Other countries in the region are also increasingly imposing restrictions on Internet content, saying that they are merely protecting vulnerable populations, such as women and children.

> **"What is particularly disturbing is that, in the war against terrorism, authorities in Asia are likely to clamp down on Internet users who have legitimate grievances, or who are exercising fundamental freedoms."**

But the danger here is that when states start to censor content considered unacceptable or harmful, they tend to open the floodgates to regulation or restriction of increasing amounts of Internet content. What is particularly disturbing is that, in the war against terrorism, authorities in Asia are likely to clamp down on Internet users who have legitimate grievances, or who are

exercising fundamental freedoms. In Burma, for instance, mere possession of a personal computer is frowned upon by the military regime. Elsewhere, such as in China, the government is moving to curtail political dissent and legitimate criticism of official policies.

The Internet is a powerful communication tool that can be used to promote equitable and just development, and to protect human rights everywhere. It should be an instrument for human advancement and the promotion of the common good of all humanity, not for stamping out the voices of those opposed to authority. At the very least, state policies and regulations with regard to Internet content and access must be the product of democratic dialogue and consultation with the affected sectors.

Australia

Internet censorship laws were passed by the Federal Commonwealth Parliament in 1999 and commenced operation on 1 January 2000. The Broadcasting Services Act was amended to give the television regulator, the Australian Broadcasting Authority ("ABA"), the power to order Australian ISPs to remove content hosted on their networks, including usenet messages. It also provides the power to to the ABA to order Australian ISPs to take-down images and text from websites and newsgroup servers on threat of fines of up to AUD$27,500 per day.

The scheme is complaints-based and information subject to banning includes material deemed unsuitable for minors (under 18 years) unless access is restricted by an ABA- approved adult verification system. Other material is subject to banning whether or not access is restricted. This includes: non-violent sexually explicit material involving consenting adults; material that depicts, expresses or otherwise deals with matters of sex, drug misuse or addiction, crime, cruelty, violence or revolting or abhorrent phenomena in such a way that they challenge the standards of morality, decency and propriety generally accepted by reasonable adults; and material that promotes, incites or instructs in matters of crime or violence.

In November 2002, the NSW Police Minister called for the banning of web sites being used to organise protests for the World Trade Organisation meeting in Sydney, claiming the sites were inciting physical attacks on the police. However, the ABA found that the sites did not breach the censorship laws that include provision for banning information that instructs, promotes or incites in violence or crime.

In November 2002, Electronic Frontiers Australia issued a report finding that the scheme had been largely ineffective. The ABA had spent most of its Internet censorship efforts investigating complaints about content on overseas-hosted websites over which it had no control. Some banned Australian websites had simply moved overseas to escape control by the national body. When Electronic Frontiers Australia requested information under the Freedom of Information Act about banned and permitted content of the same type adults are permitted to access in magazines and videos, the ABA refused. In mid 2002, the Administrative Appeals Tribunal upheld the ABA's refusal. Soon after, the Government introduced a bill that would specifically exempt information concerning administration of the censorship law from the FOIA. The bill is due to be debated by the Senate in mid 2003 and opposition parties have indicated that they will not support the Government's attempts to further prevent public scrutiny of operation of the censorship laws.

Online content censorship laws are also in force in four of the eight States and Territories. Most recently, the South Australian 'Classification (Publications, Films and Computer Games) Act' was amended. The amendments, effective from December 2002, criminalise making "matter unsuitable for minors" available online. Penalties include a fine of up to AUD$10,000. Victoria, Western Australia and the Northern Territory have had somewhat similar laws in place since 1996. A New South Wales law, almost identical to the South Australian law, was put on hold in June 2002 for re-consideration following a NSW Parliamentary Committee recommendation that it be repealed. Among other things, the Committee found that the law "could have a significant effect on the legitimate use of the Internet and may affect the fair reporting of news and current affairs".

In December 2002, the High Court ruled that Australian businessman Joseph Gutnick could sue the Dow Jones US media group for libel in Australia for an article that appeared on the website of the group's Barrons magazine, because the online article could be read in Australia. The decision upheld a ruling of the Victorian Supreme Court, that had been appealed by Dow Jones. Dow Jones' lawyer warned that the ruling was a serious precedent that would threaten online media worldwide.

The Commonwealth Cybercrime Act, approved in September 2001, includes provisions to force individuals to provide their encryption keys or decrypt data, contrary to the common law privilege against self-incrimination. In 2002, the Federal Government introduced a bill that would have allowed interception of electronic communications stored during transit (e.g.for example, email, voice mail and SMS messages) without a court order. The government was unable to obtain sufficient support in the Senate to pass the bill, and stated that it would try again at a later date. Earlier in 2002, it had been revealed that phone companies were providing law enforcement agencies with the phone call records of around 2,000 people every day, although according to the Australian Federal Police "it is not feasible to attempt to measure the number of arrests or convictions that might have eventuated" as a result of such disclosures.

References

Electronic Frontiers Australia
http://www.efa.org.au/

Cybercrime Act 2001

http://scaleplus.law.gov.au/html/pasteact/3/3486/pdf/161of2001.pdf

Broadcasting Services Act.
http://www.aba.gov.au/legislation/bsa/

Roger Clarke, Defamation on the Web: Gutnick v. Dow Jones
http://www.anu.edu.au/people/Roger.Clarke/II/Gutnick.html

Australian Privacy Foundation
http://www.privacy.org.au/

Burma

Burma is notorious as the country that has imposed the world's most comprehensive restrictions on Internet use. Burma's laws on Internet use mirror the tight control it imposes on traditional media. The government controls the country's only two TV stations, one shortwave and on FM radio station, and two daily newspapers. Although there are a number of other publications run by private journalists, these must pass the country's Press Scrutiny Board before publication. Illegal broadcasts beamed into Burma from neighbouring countries include Voice of America, the BBC World Service, and Radio Free Asia. Expatriates have, however, been active on the Net in organising opposition to Burma's military regime.

The dominant ISP is the state-owned Myanmar Post and Telecommunications (MPT), which for most of the period until 2001 was the country's only ISP. In 2001, the Burmese government began allowing limited email and Internet access, and that year 1,000 people with their own computers and modems bought government-issued email accounts. In 2002, private companies such as Bagan Cybertech, were allowed to begin selling email accounts, and by May 2003 these had acquired more than 20,000 subscribers at $60 and up for lifetime access. Even so, all Burmese Internet traffic passes through government servers, which strictly limit which Web sites can be accessed (the total is estimated at around 10,000).

Pyone Maung Maung, joint-secretary of Myanmar's e-National Task Force, told Reuters in October 2002 that the number of Burmese Internet users could rise to 200,000 in the next two years as connectivity improved. However, both local residents and expatriates believed this figure was too high because even though the government had relaxed its Internet restrictions the cost of access was prohibitive for most of Burma's 51 million people, whose average per capita income is $700 to $750 and half of whose children suffer from malnutrition. An additional hindrance: little or no local content.

In May 2003, two cybercafes opened in Rangoon, offering Burmese without their own personal computers Internet access for the first time. The cafes, owned by Fortune International Group and provided with servers by Bagan, require first-time patrons to register, giving their name, identification number, and contact address. The cafes do not allow access to free email sites such as Hotmail and Yahoo!, and patrons' Web access is subject to the same limitations as all other Burmese Web access.

The 1996 Computer Science Development Law says that possessing an unregistered telephone, fax machine, or computer modem is punishable by up to fifteen years in prison. Users can also be imprisoned for up to 15 years for "obtaining or sending and distributing any information of State secret relevant to State security, prevalence of law and order and community peace and tranquility, national unity, State economy or national culture."

In January 2000, MPT issued rules for Internet use. Internet users are banned from posting content related to politics that are "detrimental" to the country's interests or the current policies and affairs of the government. Hacking is prohibited, and users are to inform MPT of any threats they see. Users must obtain prior permission from the state-designated organisation to create Web pages, and must use only their own accounts for access. Internet access is only available by licence (granted after a written application). MPT claims the right to amend and change any of its regulations without prior notice.

References

Burma Net Regulations, January 2000
http://dfn.org/voices/burma/webregulations.htm

Computer Science Development law, 1996
http://www.myanmar.com/gov/laws/computerlaw.html

Article 19, Acts of Oppression: Censorship and the law in Burma, March 1999
http://www.article19.org/docimages/443.htm

Burmanet news
http://www.burmanet.org

Free Burma Coalition
http://www.freeburmacoalition.org

US State Department 1999 human rights report on Burma
http://www.state.gov/g/drl/rls/hrrpt/1999/282.htm

China

Internet use is growing dramatically in China, which, with 59 million online (government estimate in January 2003, 4 million of them broadband users), is now the second-biggest online population, even though that number is only a tiny fraction of its overall population of over one and a third billion people. In 2002, China also became the world's biggest mobile phone market.

Even before Internet access became available in China in 1995, the government was worried about finding ways to control what information the general population would be able to reach by its means. By 2002, it was commonly held that the country had the world's tightest Internet censorship. The country has put in place a comprehensive, nationwide filtering system that by some estimates involves as many as 30,000 people to administer. The fact that access is provided by only nine ISPs to serve the entire country, and which control the physical lines to the outside world, makes it relatively easy to apply central control.

According to Amnesty International, the government has adopted over 60 rules in the last five years to regulate use of the Internet. These include rules against disturbing state order, revealing state secrets (a very broad category that includes basic information on the government and economic statistics) and harming the countries' "honour". ISPs that do not follow these regulations can be shut down and domestic web sites that discuss political or other banned topics are taken down quickly by authorities. "Big Momas" hired by the net companies monitor web sites remove messages and report violators. Amnesty International has investigated 33 prisoners of conscience arrested for using the Internet. Many of those arrested were calling for political and legal reforms or posted information on the banned religion Falun Gong. Several have died in jail and others are reportedly being tortured.

A study carried out at Harvard from May 2002 to November 2002 found there are at least four distinct and independently operable methods of Internet filtering operating in China, with a quantifiable leap in filtering sophistication beginning in September 2002. The study's authors, who logged 19,032 Web sites that were inaccessible from China while remaining available in the US, said the blocked sites contained information about news, politics, health, commerce, and entertainment. The most commonly blocked category of sites were those about democracy, Tibet, and Taiwan; Amnesty International and Human Rights Watch are often unreachable. The authors concluded therefore that the Chinese government maintains an active interest in preventing users from viewing certain types of Web content (some, but not all, sexually explicit) and that it has managed to create effective, overlapping nationwide blocking systems that are becoming more refined over time.

The study's authors also note that the government-connected Internet Society of China (not a chapter of the international Internet Society) has asked Internet service providers and content creators to sign a pledge including self-filtering, but that few official statements document either the existence of government-maintained Web filtering or the criteria employed and thresholds necessary to elicit a block. The pledge was signed by 130 major Web portals, including US-based Yahoo.

During the summer of 2002, it was widely reported that China had tightened up its supervision of Internet use, blocking even search sites such as Google and Yahoo!, along with the BBC and sites belonging to Falung Gong and the Dalai Lama. Also that summer, according to the BBC, every Internet café in Beijing was closed for safety checks after a fatal fire; but to reopen owners had to accept tougher Web filtering as a condition of being awarded a licence. Of 2,400 cafes only 30 had reopened by September, and one top-end chain of 20 cafes, Sparkice, decided to shut down permanently. Nationwide, as many as 150,000 cafes were closed.

In September 2002, the South China Morning Post reported a significant increase in the amount of censorship being applied by the Chinese authorities, noting that although its own front page (www.scmp.com) is generally available specific stories on Taiwanese or Tibetan independence and Falung Gong are routinely blocked. The paper also reported that although the temporary ban on search engines had been lifted, searches on specific terms were blocked, requiring the user to restart the browser for any further searches, and that email containing words such as "hardcore" was bounced back to the sender. Experts note that the filtering system sharply slows Internet access for Chinese users, particularly after October 2002, when packet-sniffing software was installed to screen individual incoming and outgoing packets. All Internet traffic into and out of China must pass through one of just eight gateways. The Chinese government has also reportedly outlawed foreign software for government applications,

References

Empirical analysis of Chinese Internet filtering
http://cyber.law.harvard.edu/filtering/china/

Michael S. Chase & James C. Mulvenon, You've Got Dissent! Chinese Dissident Use of the Internet and Beijing's Counter-Strategies, Rand 2002
http://www.rand.org/publications/MR/MR1543/

Digital Freedom Network, China and the Net
http://www.dfn.org/focus/china/chinanetreport.htm

Human Rights In China
http://www.hrichina.org

Greg Walton, China's Golden Shield: Corporations and the Development of Surveillance Technology in the People's Republic of China
http://www.ichrdd.ca/english/commdoc/publications/globalization/goldenShieldEng.html

Amnesty International, State control of the Internet in China - Internet users at risk of arbitrary detention, torture and even execution, November 2002
http://web.amnesty.org/web/content.nsf/pages/gbr_china_internet

Declaration of Citizens' Rights for the Internet, July 2002
http://www.dfn.org/voices/china/netrights.htm

Pledging self-discipline
http://www.dfn.org/voices/china/selfdiscipline.htm

Measures for Managing Internet Content Provision
http://www.dfn.org/voices/china/netreg-0010txt.htm

India

The Internet in India has undergone rapid growth in recent years and regulations are currently being developed to speed up access levels in the country. Parallel to this, however, is evidence to suggest that authorities wish to develop stricter surveillance and monitoring controls over Internet activities, especially after September 11 US attacks, and the December 13 attack on the Indian Parliament.

The Information Technology Act, 2000 sets rules on cyberlaw including hacking, pornography and digital signatures. Section 67 of the Act states that anyone publishing 'lascivious' material or material that 'appeals to the prurient interest' may be jailed for up to five years. Persons convicted of hacking can be sentenced to three years imprisonment. Cybercafés and the homes of Internet users can be searched at any time without a warrant if cyber crime is suspected. Individuals can be forced to decrypt materials or face seven years imprisonment.

On 7 July 2003, the Department of Information Technology outlined an official procedure that has been declared as the first serious attempt by the Indian government to censor the Internet. Order No. GSR529(E) permits the blacking out of "websites promoting hate content, slander or defamation of others, promoting gambling, promoting racism, violence and terrorism and other such material, in addition to promoting pornography, including child pornography and violent sex''.

According to the order, various agencies — including central and state home departments, the courts, CBI, IB, police and the chairman of the National Human Rights Commission — can submit a complaint to the director of Cert-In, a new organisation which has been set up by the government to address IT security issues. This will then be examined by a committee comprising of bureaucrats from Cert-In, the department of information technology and the law or home ministry. The committee will "meet and take on the spot decision on whether the website is to be blocked or not''. Neither the producers of the website nor those with a contrary point of view are to be given a hearing. Ironically, the order also denies that the blocking is censorship: "'Blocking of such websites may be equated to balanced flow of information and not censorship.

The Parliament is currently reviewing the Communication Convergence Bill that will supercede the Information Technology Act when it comes into effect. The bill is being developed in order to address the convergence of information and communication technologies and to combine past media-specific regulations into a set of broad-based laws governing the content and transmission of all communications in India.

According to leading Indian cyber law expert, Pavan Duggal, the proposed bill gives immense powers to the new regulatory authority, the Communications Commission of India (CCI), to censor communication content by formulating programme 'codes' for content providers (Communication Convergence Bill 2001: 20.2.viii). "The basic question as to what is the fairness and impartiality in presentation of news and other programmes has been left at the subjective discretion of the CCI which has to work mandatorily under directives of the Government".

India's insurgency in border regions has prompted the authorities to clamp down on communications in areas such as Kashmir. In July 2003 it was reported that customers living in Kashmir would once again be allowed access to mobile phones services, which had previously been blocked due to "security fears".

On July 26, 2003, the Indo-Asian News Service reported that India's state-run Bharat Sanchar Nigam Ltd (BSNL) had urged the subscribers to go ahead with plans to acquire more than one telephone saying that it was not planning to disclose any data to tax authorities. The finance ministry responded by asking BSNL, the largest fixed-line service provider in the country, to disclose information about consumers having more than one telephone to ensure they file their tax returns. The company has, however, refused to compromise on its commercial policy of non-disclosure.

References

'Watch what you surf, Net police are here'
http://timesofindia.indiatimes.com

Indian Convergence Law by Pavan Duggal
http://www.cyberlawindia.com/cyberindia/convergencearticle.htm

Cyberlaws.net Cyberlaw Consultancy
http://www.cyberlawindia.com

Information Technology Act, 2000
http://www.mit.gov.in/itbill2000.pdf

The Communication Convergence Bill, 2001
http://www.naavi.org/cca_aug31/

Department of Information Technology
http://www.mit.gov.in/

The Philippines

According to one survey, over half of all Philippine Internet users live in Manila, a city which accounts for only 13 per cent of the country's population. This discrepancy is due to the fact that many parts of the country still do not have basic telephone services. Moreover, the proportion of households with personal computers remains low at 2.7 per cent.

Since 1992, mobile phone growth in the Philippines has surpassed its ASEAN counterparts to become one of the first countries where the number of mobile telephones is greater than fixed telephone lines. Mobile communications are increasingly becoming the predominant means of communication especially in the rural areas that for decades have been deprived of telephone services. The Philippines has been considered the "Text Capital of the World" with as many as 120 million text messages being sent daily by an estimated 12 million subscribers.

The Constitution provides for strong protections of freedom of speech and access to information. There are no Internet content control presently imposed by the State and anyone can publish a website without formal application.

The Students' Internet Protection Act of 2001 was filed in June 2001 and is still pending in Congress. If passed, the Act would require libraries of private and public educational institutions with Internet access to install software for blocking Internet websites displaying obscene and violent materials.

In 2000, six weeks after the Love Bug attack, the Electronic Commerce Act was enacted to enable hackers and those who spread computer viruses to be fined a minimum of $2,350 and a maximum "commensurate" to the damage caused, and can be imprisoned for up to three years.

The e-Commerce Law, while comprehensive in identifying the types of cybercrimes, does not specify particular acts punishable by law. In recognition of this, there are at least six bills pending in Congress and the Senate which aim to supplement the e-Commerce Law by specifying which acts constitute cybercrime, and to address online crimes cited in the Budapest Cybercrime Treaty. The Information Technology and E-commerce Council (ITECC) was tasked to consolidate these bills into "The Cybercrime Prevention Act of 2002".

In May 2003, ITECC formally endorsed its final version of the cybercrime bill to the Science and Technology Committee of Congress. In the draft of the bill, the crimes punishable by law include illegal access, illegal interception, data interference, system interference, misuse of devises, computer forgery, computer fraud, and offenses related to pornography and infringement of IPRs.

The Philippines' draft Anti-terrorism Bill proposes to sanction arrests without court orders, initiate 30-day detentions without charge, and sequestrate bank deposits and assets of alleged terrorists and their supporters. It would also allow the Secretary of Justice to authorize wiretaps including those of Internet communications, and probes into suspects' bank accounts. Many critics believe the bill to be a stepping-stone towards another martial law regime in the country.

References

ARTICLE 19. October 2002, Memorandum on the three Philippine Anti-Terrorism Bills, London http://www.article19.org/

International Telecommunication Union. 2002. Pinoy Internet: Philippines Case Study. ITU website http://www.itu.int/ITUD/ict/cs/philippines/material/PHL%20CS.pdf
[Accessed February 2003]

Philippine Cybercrime Bill
http://cybercrime.inmyhouse.net

Sigam, Paulynn P. Anti-Terrorism Legislation in The Philippines: A Plot of Its Own, CyberDyaryo, Manila, The Philippines, Sept. 4, 2002
http://www.worldpress.org/Asia/751.cfm

Urbas, Gregor. "Cybercrime Legislation in the Asia-Pacific Region", Australian Institute of Criminology http://www.aic.gov.au/conferences/other/urbas_gregor/2001-04-cybercrime.pdf

Singapore

With its limited size and a relatively high population density, the city-state of Singapore boasts an Internet dial-up penetration rate of 48.7% – just under half of its population accesses the Internet from home, and coverage is near 100%. The government has been actively promoting broadband Internet access, connection charges are comparatively low and schools and libraries provide easy access. Despite deregulation in 1998, the three original ISPs (of which the government owns substantial shares through a holding company) – Singnet, Pacific Internet and Starhub – still dominate the market.

However, the purposes for which its citizens can utilize this excellent infrastructure is a different story. Even before the arrival of the Internet in Singapore, the government pursued a policy of harvesting the economic benefits of media technologies while at the same time trying to limit the potential impact the free flow of information might have upon its grip on power.

Singapore was among the first Asian countries to become part of the Internet (though it did not launch a public Internet service until 1994). It was also at the forefront of imposing restrictions on what kinds of content could be accessed by its citizens. The Government has long treated the Internet as a broadcast medium and imposed the same restrictions that it does on other media. With legislation introduced in 1996 which required ISPs to curb access to websites and newsgroups the authorities deemed undesirable, the government lived up to its reputation as a nanny state. The rhetoric has since softened and the government now describes its policy as one of promoting industry self-regulation, but that is more of a euphemism for promoting self-censorship. Article 14 of the constitution of Singapore does grant its citizens freedom of expression, though it bestows the state with extensive powers to curtail that right.

The Internet Code of Practice introduced in 1996 (and amended in 1997) in Article 4 (1) defines prohibited material as "material that is objectionable on the grounds of public interest, public morality, public order, public security, national harmony, or is otherwise prohibited by applicable Singapore laws." The Singapore Broadcasting Authority (SBA) was set as the regulatory body for the Internet in 1996. It has repeatedly emphasized that it does not regulate or monitor personal Internet communications such as IRC or email.

The regulator has in the past concentrated on ordering ISPs to filter mainly high-volume pornographic websites and newsgroups. What is a matter for concern, however, is that the 'promotion' of homosexuality and lesbianism is listed in the Internet Code of Practice as prohibited content next to the depiction of incest, paedophilia, bestiality and necrophilia.

The protection of children from unsuitable content on the Internet is the SBA's main argument for its monitoring activity. The other aspect of the state's paternalistic approach is the concern for ethnic and religious harmony in Singapore. Its' favorite metaphor is that of health and disease, and in December 2002 the "Cyber Wellness Task Force" was formed to "inculcate the right values and a healthy Net culture among Singaporeans," especially the young.

In January 2003 the SBA was merged into the new Media Development Authority (MDA) with the aim of promoting the growth of the Singaporean media industry. and, as was the case under the SBA before, a distinction is made between Internet Content Providers (ICP) and Internet Access Providers (IAP).

ICPs who either offer a subscription news service, publish websites with political or religious content pertaining to Singapore, or operate a website as a political party, must register with the MDA and are held liable for the content of their websites. IAPs must also register with the MDA, but with the IAPs the regulator operates a 'light-touch' approach, 'allowing' them to curtail access to prohibited material once alerted to its existence by the authority and not explicitly requiring them to undertake proactive screening of content.

The government has also made extensive use of civil defamation suits to silence its opponents – a practice that according to Amnesty International could have an even more insidious effect on freedom of speech than the Internal Security Act (ISA). In July 2002 police investigated a prominent leader of the Muslim organisation Fateha over allegedly defamatory articles that had been posted on its website Fateha.com. He now faces charges of sedition.

The 1998 Computer Misuse Act prohibits unauthorised interception of Internet communications. The same law in Article 15 gives the police wide-reaching powers to access any computer and its data upon the mere suspicion that an offence has been committed with it, and also requires users to provide decryption information to the police. A ban on the import of data encryption technology was lifted in 2001.

Producers of Internet content are most welcome to operate their business in Singapore free from restrictions as long as that content is broadcast

outside of Singapore or is not of a political or religious nature. Singapore's excellent ITC infrastructure is intended by the government to bring economic prosperity to the country, not to bestow on its citizens the right to express dissenting opinions.

References

Media Development Authority (MDA) policy & regulations
http://www.mda.gov.sg/medium/internet/internet.html

ITC Statistics provided by the IDA
http://www.ida.gov.sg/Website/IDAContent.nsf/dd1521f1e79ecf3bc825682f0045a340/2d393fa3f37245c8c82568390001f755?OpenDocument

ITU 2001 case study on the Internet in Singapore
http://www.itu.int/asean2001/reports/material/SGP%20CS.pdf

Anil S, 'Re-Visiting the Singapore Internet Code of Practice', 2001 (2) The Journal of Information, Law and Technology (JILT)
http://elj.warwick.ac.uk/jilt/01-2/anil.html

Computer Misuse Act, 1998
http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan002107.pdf

Alternative non-government sources of information and discussion on Singapore
http://www.singapore-window.org

http://www.geocities.com/newsintercom

http://www.thinkcentre.org

South Korea

After the country was damaged by an economic crisis in the mid-1990s, the Korean government declared that one solution for reviving the economy lay in the development of ICTs. What followed was a widespread restructuring and the development of policies to promote ICTs, as well as the construction of a nation-wide, high-speed telecommunication network. Due to such efforts, the industry has developed significantly with the result that by November 2002 the number of high-speed Internet Broadband subscribers exceeded 10 million.

Korea was one of the first countries to adopt a law limiting free speech on the Internet. In 1995, The National Assembly amended the Electronic Communication Business Law to include a new provision on the "regulation of dangerous communications." It authorised the Ministry of Information and Communication to regulate "dangerous communications" and delegated the regulatory power to the Information and Communication Ethics Committee (ICEC). The regulation has been used to block websites of the anti-military movement, homosexual rights and school dropouts.

In 1999, a user who had posted an opinion about a battle a few days earlier between the South Korea and North Korea navies in West Sea of Korea was blocked from logging onto his account by order of the Ministry and his article was removed. He took the matter to the Constitutional Court, which on June 27, 2002, ruled that the "dangerous communications" provision of the law were unconstitutional because it violated freedom of speech. In November, 2002, the National Assembly amended the law to now regulate "illegal content". Under the revised law, the MIC can control and delete illegal content on the Internet without any approval or agreement from the court.

The 2001 Ordinance of the Act on Promotion of Utilization of Information and Communication Network compels webmasters to use PICS to label harmful content designated by ICEC. ICEC decides what is harmful content under the Youth Protection Act, which classifies gay and lesbian content as "harmful to youth". ICEC has designated www.exzone.com, a homosexual website, as harmful on the grounds that it encouraged homosexuality and carried obscene information. The operator of the site and a federation of 15 gay rights associations filed a suit against the government in January 2002 stating that the law violated the constitutional right to free speech. The case is still pending.

The National Security Law gives broad powers to the government to restrict speech and to prevent support or discussion of North Korea. In June 2002, police arrested Kim Kang-pil for posting messages related to North Korea on the Democratic Labor Party's website. The government claimed his actions violated the National Security Law, Article 7, Clause 1 (an act advantageous to the enemy) and Clause 5 (bringing the materials of profit to the enemy). The first court sentenced him to one year's imprisonment. Kim appealed and was released in December 2002 after the appellate court suspended the sentence for two years. On July 11, 2003, police arrested and restricted Kim, Yong-chan and Kim Jong-gon for possessing books The Captal written by Karl Marx, For Marx by Louis Althusser and The Imagination of the New Left by George Katsiaficas and uploading materials on their Internet community bulletin board about these books and Manifesto of the Communist Party from 1948. This case now is pending.

Copyright law is also used to suppress speech. A group of workers who were opposing a merger of their company to POSCO the largest iron company in Korea, set up a website 'ANTIPOSCO' which was designed in a similar style to POSCO's original website. On April 17, 2000, a court issued a preliminary decision requiring ANTIPOSCO to shut down, accepting POSCO;'s claim that it violated their copyright. This decision was later cancelled in July 2001.

There is also continuing controversy about police access to information on users' identity. On July 2003, police requested the Korean Confederation of Trade Unions (KCTU) to reveal the identity of the user who uploaded material friendly to North Korea on the internet bulletin board of KCTU website. This request was made under the Protection of Communication Secrets Act, which permits police to request ISPs to reveal without a court warrant the identification of people who use the network. According to Jinbonet, which provides 650 social groups and trade unions with Internet hosting, the police had requested it to reveal user's identification without any warrant from the court about twice a month. Jinbonet has refused the requests and in May 2002 sued to challenge this law in the constitutional court.

On March 2003, MIC proposed rules to facilitate real identification by compelling the use of National ID number of Korean people before they would be permitted to post on the bulletin boards of all public organizations.

References

International Telecommunications Union statistics report, 2001
http://www.itu.int/ITU-D/ict/statistics/

The Lesbian and Gay Alliance Against Discrimination in Korea
http://outpridekorea.com/lgaad

Jinbonet and the Progressive Network Center
http://english.jinbo.net

Citizens Coalition for Media Watch
http://www.mediawatch.or.kr/

Ministry of Information and Communication
www.mic.go.kr

Ruling the Electronic Communication Business law to be unconstitutional
http://www.base21.org/show/show.php?p_docnbr=21832

Declaration to refuse the Internet Contents Rating System
http://www.base21.org/show/show.php?p_docnbr=21120

Don't use the National Security Law to suppress the Internet!
http://www.base21.org/show/show.php?p_cd=209&p_dv=0&p_docnbr=22659

Thailand

According to an estimate by the National Electronic Computer Technology Center in mid-2003, there are currently 6 million Internet users in Thailand, almost double the number of users estimated in the previous year. This translates to about 10% of the Thai population who use the Internet in some form. The geographic distribution of Internet users is very uneven, with the overwhelming majority of users living in Bangkok and the major cities.

Internet access is provided by 18 commercial ISPs and 4 non-commercial Internet hubs. Until March 2000, the Communications Authority of Thailand had been licensing ISPs, which had to hand over to CAT 32% of their shares upon receiving a licence. Awaiting the appointment of a new regulatory body for the Internet, CAT has ceased to grant any more licences. CAT also controls the country's only international Internet Gateway linking Thai users to international sites.

The current ICT minister has stated that access to information is a fundamental human right, and there are various schemes in place to improve Internet access to citizens across the country. This promotion of IT development through state-operated ISPs ñ as welcome and necessary as it is ñ comes with a potential problem: The state authorities seem to see it as their duty to protect their citizens from information that they themselves deem undesirable. The subsidised nationwide ISPs such as Schoolnet and CleanNet do not provide unlimited access to the Internet, ostensibly to protect children and family values. This leads down the path of a controlled access to the Internet for Thai citizens, especially the poor and rural people.

The current 1997 constitution has been widely praised for its provision of both Freedom of Speech and Access to Information. Several older laws that contradict the constitution have not yet been repealed, and the National Telecommunications Commission (NTC) ñ which will be responsible for licensing and the regulation of Internet service providers ñ has not yet been implemented. Information Technology Laws such as a Data Protection Law and a Computer Crime Law are being developed by the National Information Technology Committee under the Prime Minister's office, but have yet to be presented to parliament. There is therefore currently no specific regulatory body or legal framework to deal with Internet communication. Legislating for e-commerce has been a priority for the Thaksin government, and in 2002 the Electronic Transactions Act was passed which recognizes electronic signatures and allows for data encryption. The draft Computer Crime Law includes provisions for ISPs to retain communications data for three months and would allow state agencies access the data and demand keys to encrypted data ñ measures which the government declared as policy in 2001.

In 2002, the National Police Office set up a form on which citizens can report obscene or defamatory websites. In its first year, 7,700 websites were reported, almost 70% for pornography, 5% for child pornography and 7% for posing a threat to national security. It is not clear in how many cases the police have taken action. Police also sent letters to Thai and international ISPs in 1999 telling them to shut down websites that contained fake nude images of Thai actresses.
There have been attempts by state authorities to limit access to websites operated by a Malay Muslim separatist group, PULO. In 1999, Thai police approached a US-based webhost requesting that the PULO site be shut down, and in 2002 it ordered a Thai ISP to block access to the site, resulting in URL requests being redirected to the above mentioned police website. This blocking lasted only a couple of days.

Since the formation of an Information and Telecommunications Ministry in 2002, efforts to control Internet content have continued. In December 2002, the ICT minister, Surapong Suebwonglee attempted to force ISPs to censor pornographic and 'subversive' content on websites by threatening to cut their interconnections through CAT.

Since July 2003 over 100 sites have been blocked by Thai ISPs. This "agreement" was made with the ICT ministry after it was made clear that the ISP's licences could be at risk if the block was not implemented. The ICT ministry is currently setting up a website ratings system which would ban not only child pornography, but also terrorism-related information, derogatory remarks about religions or the Thai royal family, and possibly even betting information.

Lese majeste is a pet topic of freedom-of-speech reports on Thailand, but is also something of a red herring. While it does limit freedom of speech and is occasionally used to discredit political opponents, it is not high on the agenda of most Thai Internet users in the current situation. Webboards have been popular for political debate and although some observers have suggested a trend towards more caution over the last two years, there has been no overt attempt by state authorities to censor webboards. In fact, they become the outlet for public debate when other mainstream media are censored, including the webboard of the ICT ministry itself.

In July 2003 the ICT ministry 'requested' that the four companies providing online-gaming networks in Thailand impose a curfew on the popular online game, Ragnarok. The providers agreed to the ministers' request/demand and servers are now inaccessible between 22:00 and 06:00. The motivation for this curfew had been increasing worries over children and teenagers becoming addicted to Internet gaming. The curfew will come up for review in September 2003, but the IT minister is considering a registration scheme which would require online gamers to register with their national ID cards to allow them to continue playing at night. While such a scheme would allow for surveillance of individual computer users by state agencies, it is not clear how children could be stopped from 'borrowing' adults' IDs in order to continue gaming at night.

References

List of Thai ISPs
http://www.cat.net.th/isp/

Map of Thai Internet Structure
http://www.cat.net.th/Internetmap/Internetmap.html

NECTEC Statistics and Reports on the Internet in Thailand
http://ntl.nectec.or.th/Internet/index.html

Policy documents and law texts on the NICT website (mostly in Thai)
http://www.nitc.go.th/document/publications.html

National Information Technology Committee
http://www.nict.go.th/

Information and Telecommunications Ministry
http://www.ict.go.th/

National Electronic Computer Technology Center
http://www.nectec.or.th/

Communications Authority of Thailand
http://www.cat.net.th/

ITU 2002 report on Internet in Thailand
http://www.itu.int/ITU-D/ict/cs/thailand/material/THA%20CS.ZIP

The National Police Office Website
http://www.police.go.th/crimewebpost/report/sum.php

Internet censorship in Europe

Regional report

Europe has 23 percent of the global Internet universe, behind the US with 29 percent and well ahead of Asia with 13 percent. Just as individual nations have a digital divide, so does Europe as a whole. In general, the trend is for Internet penetration to decrease from north to south and west to east. The highest levels of connectivity are to be found in Scandinavia, followed by the UK, Germany, and France, and the lowest levels are to be found in countries like Spain (whose number of Internet users is now growing fast), Italy, and Greece, following the same pattern as computer penetration. Among Eastern European countries, Estonia, whose Internet penetration is similar to that of leading Western countries, is the leader. The pattern of adoption of broadband is also uneven due to the wide variation in quality of telecommunications infrastructure and national regulatory policies. In the UK, for example, broadband subscribers did not reach 1 million until 2003 due to high prices from the monopoly wholesaler of DSL, British Telecom, which balked at cannibalising its lucrative leased line and ISDN businesses; by comparison, Germany's Deutsche Telekom's low prices rapidly created a much larger market. Geography plays a role, too, as countries where the population is largely rural cannot make use of either cable or DSL technologies and must rely on satellite and fixed wireless as these become available.

> **"In general, the more liberal a country's laws were before the 9/11 attacks, the more likely they are to have changed."**

The bust of the telecommunications market since the stock market peak in 2000 means there has been a lot of consolidation and cross-ownership. Telcos burdened with debt are tending to consolidate, and the likely outcome will be a relatively small handful of pan-European operators. Candidates to be among that handful include: the US's AOL, Spain's Terra Lycos, France's Wanadoo (which owns Britain's Freeserve and is owned by France Telecom), and Italy's Tiscali.

In general, the more liberal a country's laws were before the 9/11 attacks, the more likely they are to have changed.

The leading body for settting policy in Europe is the European Union (See the EU entry on page 67). Although strictly speaking EU legislation applies only to its member states, it has a much farther reaching effect because so many countries want to join. Ten new countries – Slovakia, Slovenia, Latvia, Lithuania, Estonia, the Czech Republic, Poland, Hungary, Cyprus, and Malta – are set to become member states in 2004, and three more – Bulgaria, Romania, and Turkey – are seeking acceptance. The most important Western non-member is Switzerland; other holdouts include Norway, Iceland, and Lichtenstein. Countries that do wish to join the EU are required to reform their laws to harmonise with the EU's. Yet even the laws of countries that have no plans to join, like Switzerland (which is a signatory to the Cybercrime convention), are tending to head in the same direction as the EU's; Switzerland, for example, has already mandated data retention for a period of six months, and new structures set up since 2001 police the Internet for illegal content. Norway, although it voted against joining in 1994, has implemented the full set of EU directives as a member of the European Economic Area. Turkey, for example, is reviewing its laws on freedom of expression, as these will need to be relaxed to fit the criteria of Article 10 of the ECHR.

> **"Many countries, including Spain and Russia, have structures in place to allow censorship of the Internet, if only to combat child pornography."**

Once directives are accepted at the EU level – such as the EU Copyright Directive (2001), EU Electronic Commerce Directive (2000), or the EU Data Protection Directive (1995) – they must be implemented in national legislation by each member state within a time frame specified in the directive itself, typically three years, although the EUCD allowed member states only 18 months. National legislatures do not always interpret the directive in the same way, and debate at the national level over specific provisions may be intense. The EUCD is a good current example: Denmark already had some similar provisions on its books, but in the UK the EUCD is highly controversial and has yet to be implemented. Only Greece and Denmark met the deadline for passing supporting legislation for the EUCD. Therefore, despite the intention to create a consistent framework there are often national variations that reflect cultural, political, and social

differences between the diverse countries that make up the EU.

The Council of Europe is also influential (See the COE entry on page…). Nearly every nation has signed and implemented the Data Protection Convention (Treaty 108 of 1980). Most countries have signed the Cybercrime Convention, with Turkey being the notable exception. However, no EU countries have ratified it. Many countries, including Spain and Russia, have structures in place to allow censorship of the Internet, if only to combat child pornography. Slowly, European countries seem to be converging on a standard under which ISPs are not liable for content they host unless they fail to take it down when notified it is illegal. Many, such as Denmark extend their laws governing offline media to the Internet.

> **"Data retention laws are sweeping the continent, beginning with Belgium, which adopted a law requiring ISPs to retain user data for up to 12 months as long ago as 2000."**

Data retention laws are sweeping the continent, beginning with Belgium, which adopted a law requiring ISPs to retain user data for up to 12 months as long ago as 2000. Other countries adopting data retention laws include Denmark (as part of its 2002 anti-terrorism act), Anonymous use of the Internet is also under threat, although few countries have gone as far as Belgium, which passed a law in 2001 forbidding it. Also popular are laws requiring ISPs to install (usually at their own expense) equipment to make it possible for police to surveille their users; such laws have been passed in Bulgaria, Hungary, and Russia. Data retention is being debated in the UK, where ISPs have protested against the government's proposed data retention rules under the Anti-Terrorism, Crime and Security Act (2001), partly on the grounds of cost, but also on the grounds of privacy.

There is increasing similarity between EU and US law, even in the area of privacy. The UK in particular has long claimed a "special relationship" with the US. In the past, this pulled UK policy away from the EU's in some significant areas. For example, the wars over the legalisation of strong cryptography saw the UK hew closely to the US line. Cryptography now is legal in most European countries, although its use and manufacture have been banned in Belarus and Russia since 1995. In the UK, police may demand a copy of the key necessary to decrypt user data under the Regulation of Investigatory Powers Act (2000).

> **"Another trend throughout Europe is blamed on US pressure, but has its roots in government desires that had no public acceptance until the 9/11 attacks: the advent of biometric systems for authentication and identification"**

Another trend throughout Europe is blamed on US pressure, but has its roots in government desires that had no public acceptance until the 9/11 attacks: the advent of biometric systems for authentication and identification. The US portion of this is the Enhanced Border Security Act, which mandates that all visa-waiver countries must begin issuing biometric passports by October 2004; otherwise their citizens will have to apply for visas to visit the US. The International Civil Aviation Organisation has settled on a contactless chip in the passport that will store a facial scan from which a template can be drawn to meet the requirements of any facial recognition system that needs to read the chip. There will also be room for a second biometric of the individual nation's choice on the chip; the UK is expected to choose an iris scan, in line with its proposals for national ID cards.

But biometric travel documents are only the beginning. Biometric systems are coming into use to secure staff areas in airports such as London City and Israel's Ben Gurion, as season passes for Germany's Hanover zoo, as guarantors of identity for asylum seekers, and as electronic signatures for banks beginning with the UK's Nationwide Building Society. The 9/11 attacks are the driving force only behind the travel systems; the others are primarily about reducing fraud. But it is not clear what will happen to the data stored by these systems.

European Union

The European Union is made up of 15 member states from Western Europe (expanding to 25 in 2004) based in Brussels and Strasbourg with a combined population of some 377 million. They are bound together by a series of treaties into a quasi-federal system where decisions made by the EU are adopted by the member states.

One of the challenges in understanding the EU lies with keeping track of the number of interlocking organisations (many with similar names) that govern it. Effectively, the EU is governed by a three-branch system of Commission, Council, and Parliament, with the Court of Justice and the Court of Auditors to respectively interpret the law and handle the finances.

The Council of Ministers is the EU's main decision-making body, regularly bringing together ministerial representatives of the member states; it is also the body that coordinates the activities of member states, handles international agreements, and makes decisions relating to foreign and security policy. Members take it in turn to hold the EU presidency for six-month terms.

The European Parliament is elected every five years by universal suffrage, and is made up of representatives from each EU member country. The Parliament shares both legislative power and budgetary authority with the Council of Ministers, and exercises democratic supervision over the European Commission.

The European Commission presents legislative proposals to the European Parliament and the Ministers, works with the Court of Justice to ensure that EU law is properly applied, and acts as a guardian of the treaties. It is made up largely of civil servants representing the member states, and it works out the detailed procedures for implementing directives in closed meetings without publishing minutes. This secrecy is an area of dispute between the European Parliament and the Ministers on one side, and the EC on the other.

There are three kinds of law within the EU. For the purpose of discussing Internet rights, the most important is the secondary legislation drawn up in the form of directives by the Ministers. Also important are the primary legislation, treaties, which are drawn up on the basis of direct negotiations between member states' governments, and must be ratified by national Parliaments (though not by the European Parliament). The implementation of directives, which are binding upon member states as to objectives and deadline, is left to the statesí national legislatures.

Key EU efforts over the last few years have included the Data Protection Directive (95/46/EC); the Directive on Privacy and Electronic Communications (2002/58/EC), and the proposed EU Council Framework Decision on attacks against information systems (2002/0086 (CNS)). The Data Protection Directive took EU law strongly in the direction of "opt-in" so that consumers' data can't be used without their specific consent. This directive has been adopted by all member states. Probably its most controversial clause, at least outside the EU, is the one barring the transmission of data to countries without similar protection in place; the most significant of these countries is the US, which protested strongly against the European law. These issues have resurfaced with respect to the US's proposed CAPPS-II programme, which seeks to use a variety of databases to perform background checks on all passengers flying into the US. This was also a source of disagreement within the EU's own internal governing structure, as the Ministers proposed to comply with these US demands and the European Parliament publicly opposed doing so.

There have been a number of other, similar disagreements between the Parliament and the Ministers on issues concerning privacy and civil liberties.

The EU has also modified or adopted a number of specific measures for combating terrorism since the 9/11 attacks. In 2002, the European Union adopted a new directive on telecommunications privacy (2002/58/EC) replacing one from 1997 to more clearly extend it to new communications technologies. It limits spam. Its' most controversial provision, which was strongly pushed by the US, allows members states to adopt laws on data retention. Since then, the Danish and Belgium presidencies have worked on adpting a framework decision on data retention that would require member states to adopt these laws.

The proposed Council framework decision on attacks against information systems, intended to tackle cybercrime, requires member states to establish in national law the criminal offences of illegal access to and interference with information systems. It also contains provisions on criminal penalties, rules on liability of legal persons and associated sanctions, rules on jurisdiction, and a requirement for member states to join the existing network of operational points of contact. The Parliament delivered its opinion on the draft framework decision in October 2002, and the Council reached political agreement on the text of the main articles on 28 February 2003. Also in February 2003, the Commission proposed a European Network and Information Security Agency to serve as an advisory centre on the

subject of cybersecurity. Member states began to consult on implementation in mid 2003.

The EU Copyright Directive was accepted in 2001 with an 18-month deadline for member states to pass supporting legislation. The EUCDís provisions are similar to the US's Digital Millennium Copyright Act. The EUCD makes it illegal to circumvent copyright protection measures without reference to whether that circumvention enables a violation of copyright, and makes circumvention tools illegal. The effect will be to endanger cryptography research and - opponents such as Eurorights argue - help turn big software and media companies into even bigger monopolies.

For the past several years, the European Union has been promoting access and e-government as part of its eEurope2002 strategy. Most member state in the EU have high rates of Internet penetration, especially the northern countries. An updated eEurope 2005 Action Plan was approved by the Commission in May 2002. The 2005 Plan calls for "the widespread availability and use of broadband networks throughout the Union by 2005 and the development of Internet protocol IPv6 (as well as) the security of networks and information, eGovernment, eLearning, eHealth and eBusiness." This will include a focus on "modern online services" such as e-government, e-learning, and e-health. In the Central and Eastern European (CEE) region, the EU has promoted the much more modest eEurope+ Action Plan which focuses more on access and less on services.

A new proposal ("Regulation Of The European Parliament and The Council on the Law Applicable to Non-Contractual Obligations ("Rome II")) created with the purpose of harmonising conflict rules could open the way to allowing people in one country to sue a newspaper in another country under the laws of the reader's country of origin (a similar approach was considered at one time for disputed ecommerce transactions). Such a law would make most Web-based publications economically unfeasible, as they would be liable under a host of national laws instead of just their own.

References

Explanation of EU government organisational structure
http://europa.eu.int/inst-en.htm

Explanation of decision-making process in the EU
http://www.eurim.org/EURGUIDE.html

Cyber-Rights & Cyber-Liberties (UK) Cybercrime Pages
http://www.cyber-rights.org/cybercrime/

IRIS, Cybercrime Dossier
http://www.iris.sgdg.org/actions/cybercrime/

Global Internet Liberty Campaign
http://www.gilc.org

Eurorights (online rights, primarily copyright)
http://www.eurorights.org

Statewatch (human rights group covering surveillance issues)
http://www.statewatch.org

List of measures adopted to counter terrorism since 9/11
http://www.eurunion.org/partner/EUUSTerror/2002EURespUSTerror.htm

Proposal ro harmonise the conflict rules
http://europa.eu.int/eur-lex/en/com/pdf/2003/com2003_0427en01

Council of Europe

The Council of Europe, is a Strasbourg-based treaty organization of 45 countries. Since its creation following the Second World War, the organisation has promoted human rights and democracy. Its most important success is the European Convention on Human Rights and the creation of the European Court of Human Rights. In 1980, it released a treaty on privacy and data protection that set international standards. The COE has also promoted media and freedom of information and expression.

However, in the past 15 years, the CoE has shifted its focus and has increasingly promoted surveillance and public security interests over human rights. The CoE has created an international Convention on Cybercrime, which calls on countries to adopt extensive new surveillance powers, create new crimes and to share information. The CoE is also promoting Internet censorship.

In September 1995, the Council of Europe approved the Recommendation of the Committee of Ministers to Member States Concerning Problems of Criminal Procedure Law Connected with Information, No. (95) 13, It called on countries to adopt laws to make telecommunications systems wiretap ready and limit the availability of encryption technologies.

In 1997, the Council of Europe formed a Committee of Experts on Crime in Cyber-space (PC-CY). The group met in secret for several years drafting an international treaty. The Committee was made up of representatives selected by governments (mostly law enforcement officials). No industry, user or civil liberties groups were allowed to participate.

The text of the draft convention was strongly criticised by a wide spectrum of stakeholder groups. Privacy and civil liberties advocates condemned its promotion of surveillance and its lack of controls such as authorisation requirements and the absence of dual criminality provisions. Prominent security experts criticised it because of previously articulated limitations on security software. Industry expressed concern because of the costs of implementing the requirements, and the challenges involved in responding to requests from dozens of different countries. Following these criticisms a few drafts were released starting in April 2000 but no major changes were made. In November 2001 the Convention was signed by 30 countries.

The convention comprises three sections. Part I proposes the creation of new crimes that affect the use of computers including hacking, copyright, distribution of child pornography, and computer fraud. Part II requires countries to enact new laws to increase their domestic surveillance capabilities, especially of the Internet. This includes the power to intercept internet communications, gain access to traffic data in real-time or through preservation orders to ISPs, and creating access to secured or "protected" data, which may include encryption keys. There are detailed requirements for countries to follow but no corresponding protects to prevent abuses. The third part of the treaty requires all signatory states to cooperate in criminal investigations and allow for surveillance and search powers to be used, even when the activity is not a crime in the territory conducting the investigations.

After the terrorist attacks on the United States, the Convention was positioned as a means of combating terrorism. The Convention will come into force once ratified by five signatories states, of which three must be members of the Council of Europe. Thus far, it has been signed by 32 countries (including the United States, Canada, Japan and South Africa) but has only been ratified by 2 countries, Albania and Croatia. Japan is currently considering its position on ratification. Once the Convention is in force, other non-COE countries like China and Singapore can also ask to join. The Australian government announced in July 2001 that its bill on computer crime (since enacted), which requires users to provide encryption keys, is based on the Convention.

In November 2002 the CoE adopted the Additional Protocol to the Convention on Cybercrime concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. The protocol calls on countries to criminalise speech, including online "insults" based on various criteria.

The CoE Council of Ministers also recommended in November 2001 that the committee develop a protocol on "terrorist messages and the decoding thereof." The status of this proposal is unclear and the CoE denies that it is actively working on the proposal.

The CoE Council of Ministers approved a "Declaration on Freedom of Communication on the Internet" in May 2003. It calls for the use of filters in schools and removal of content and blocking of web sites "for the protection of minors,". It says that ISPs should be held liable for their users' content if they host web sites and do not immediately remove the material when notified. The statement also recommends that web sites should not have to be licensed and that users should have the right to be anonymous but

at the same time says that states should be able to identify them.

A group of specialists is also drafting a requirement that all web sites provide a "right of reply." It would extend the traditional media requirements to allow any person who feels aggrieved to force web site operators to place his response online on their site. Experts point out the problems both with applying this requirement to a more dynamic environment run by much smaller organizations than mass media groups and its with its potential for abuse.

References

Council of Europe Homepage
http://www.coe.int

Recommendation of the Committee of Ministers to Member States Concerning Problems of Criminal Procedure Law Connected with Information, No. (95) 13
http://www.privacyinternational.org/intl_orgs/coe/info_tech_1995.html

Convention on Cybercrime, ETS No. 185
http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Combating_economic_crime/Cybercrime/

Protocol on Hate Speech, PC-RX (2002) 24
http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Combating_economic_crime/Cybercrime/Racism_on_internet/

Declaration on Freedom of Communication on the Internet, Strasbourg, 28 May 2003
http://www.coe.int/t/e/human_rights/media/5_Documentary_Resources/1_Basic_Texts/2_Committee_of_Ministers'_texts/PDF_H_Inf(2003)007_E_CMDec_Internet.pdf

Draft Recommendation on the right of reply in the new media environment, 25 June 2003
http://www.coe.int/T/E/Human_Rights/media/7_Links/Right_of_reply_hearing.asp

Privacy International Cybercrime Page
http://www.privacyinternational.org/issues/cybercrime/index.html

Treaty Watch
http://www.privacyinternational.org/issues/cybercrime/index.html

Cyber-Rights & Cyber-Liberties (UK) Cybercrime Pages
http://www.cyber-rights.org/cybercrime/

IRIS, Cybercrime Dossier
http://www.iris.sgdg.org/actions/cybercrime/

Global Internet Liberty Campaign Member Letter on Council of Europe Convention on Cyber-Crime Version 24.2, December 2000
http://www.gilc.org/privacy/coe-letter-1200.html

Austria

Internet censorship is generally limited in Austria. In 1997, all the major ISPs took themselves offline voluntarily for 24 hours to protest the police seizure of all of the equipment belonging to the ISP V.I.P., following a year-old tip from German police about a pornographic post by a former user. However, since then, nothing of that naure has occurred. Even Samizdat publishing like that practiced by the Internet rights group quintessenz (www.quintessenz.at) has attracted no countermeasures. quintessenz publishes a database containing a fast-growing collection of mostly non-public surveillance-related documents by EU police, telecoms, standards groups and telecom suppliers, including projects such as Enfopol.

The Ministry of Interior and the Internet Service Providers Association run hotlines for reporting child pornography and neo-Nazi content. Austria signed the Council of Europe Cybercrime Convention in November 2001 but has not yet ratified or implemented it. Austrian President Thomas Klestil signed the Cybercrime Hate Speech Protocol on 30 January 2003.

The key events of 2002 were all closely related to surveillance. In January 2002, the Überwachungsverordnung [UEVO] law went into effect, despite the protests of telecommunications operators, ISPs and civil liberties groups. The UEVO is the Austrian operational/technical implementation of the ENFOPOL surveillance plans. Mobile phone companies have filed suit against the UEVO in the Austrian Supreme Court of Justice. In addition, the Ministry of Transport, Innovation and Technology is currently drafting a Law of Communications which may require data retention. The government claims that "there is a basic readiness on the part of providers to agree to the introduction of the obligation." The Austrian Federal Constitutional Court ruled in February 2003 that the government must pay telecommunications providers for any changes in their networks that make them wiretap ready.

In June 2002, two members of Parliament (both high-ranking army officers, one of them a self-declared "German" nationalist and far-right "freedom party" FPOE member) pushed through Parliament without discussion a rider to the new "Militärbefugnisgesetz" bill giving the military additional powers. This allows army officials to demand an undefined amount of personal user data from telecommunications companies, without any requirements or restrictions.

References

Advisory Council for the Internet and the New Media
http://www.bka.gv.at/bka/medien/bin.htm

Internet Ombudsman
http://www.ombudsmann.at/

Protest against the military coup concerning surveillance
http://www.vibe.at/aktionen/200206/mil_18jun2002.html

ARGE Daten on the new surveillance laws
http://www.ad.or.at/news/pw20020516.html

quintessenz collection of surveillance documents
http://www.quintessenz.org/cgi-bin/index?funktion=view&id=000100002333

Austrian Data Protection Commission
http://www.bka.gv.at/datenschutz/

European Union Council Survey on Data Retention, November 2002
http://servizi.radicalparty.org/data_retention/index.htm

Initiative der Republik Österreich zur Annahme des Beschlusses des Rates zur Bekämpfung der Kinderpornographie im Internet
http://www.bka.gv.at/bka/medien/auinitiative.pdf

Ueberwachungsverordnung
http://futurezone.orf.at/futurezone.orf?read=detail&id=104892

Decision of Austrian Federal Constitutional Court, February 27, 2003
http://www.epic.org/privacy/intl/austrian_vfgh-022703.html

Belgium

The Constitution provides extensive protection of privacy and free speech but over the past few years a series of laws have been adopted that limit those rights.

The Parliament adopted the Computer Crime Act in November 2000. This law requires ISPs to retain users' communications data and subscriber information for a minimum of 12 months. An implementing regulation defining the type of data and the length of time that it will be kept for has not yet been adopted but the Belgium police are demanding retention for 3 to 5 years. The Privacy Commission must be consulted before the decree is implemented. The law also requires network managers or experts to assist with decrypting encrypted messages. However, a 1994 law that limited the use of encryption was repealed in 1997. Belgium has signed the Council of Europe Cybercrime convention but has not ratified it or amended the Computer Crime Act. The Government signed the COE Cybercrime Hate Speech Protocol on 28 January 2003.

Another law adopted in December 2001 prohibits the anonymous use of telecommunications networks. A Royal Decree issued for the law allows the banning of services that do not identify the user. In October 2002 the government announced that all citizens would be issued a new national ID card with a digital certificate to encourage Internet transactions with both government and private sectors.

In 1999 the Internet Service Providers and the Federal Police signed a "Cooperation protocol in order to combat illegal acts on the Internet" with a view to establishing a Central Point for complaints about child pornography. ISPs are not required to search their content but they must inform the police if illegal material comes to their attention. ISPs must prevent access to the material if the Central Point determines that the material is illegal.

Starting in 2000, the International Federation of the Phonographic Industry, the music trade association began tracking users who use peer-to-peer software to transfer music and other files. ISPs provided the names of their users under a "gentleman's agreement." Some names were passed onto police for prosecution. In November 2001 the practice was strongly criticised by the Data Protection Commission.

References

Interdisciplinary Centre for Law and Information Technology
http://www.law.kuleuven.ac.be/icri/

Droit & Nouvelles Technologies
http://www.droit-technologie.org/

Centre de Recherches Informatique et Droit
http://www.droit.fundp.ac.be/crid/

Association Electronique Libre
http://www.ael.be/

Police Fédérale, Point de Contact Judiciaire
http://www.gpj.be/index2.html

Protocole de collaboration pour lutter contre les actes illicites sur l'Internet
http://www.ispa.be/fr/c040202.html

Commission de la protection de la vie privée
http://www.privacy.fgov.be/

Internet Rights Observatory
http://www.internet-observatory.be/

Big Brother Awards Belgium
http://www.internetaddict.be/dossiers/bigbrotherawards/bigbrother_fr.asp

Internet Key Facts 2002
http://www.ipb.be/upload/album/AP_1441.pdf

EPIC and Privacy International, Privacy and Human Rights 2002, Belgium
http://www.privacyinternational.org/survey/phr2002/

Czech Republic

The Charter of Fundamental Rights and Freedoms provides for extensive freedom of speech and privacy rights. There are no resolutions related specifically to Internet censorship and there are no cases of web sites blocked for political or religious reasons. The act of censorship in general is illegal.

Internet penetration is around 12 percent. In the recent (July 2003) TNS Factum survey, 36% of respondents had connected to the Internet at least once during the last month. 56% of them were man, 44% woman. 47% were under 29, 27% 30 – 44, 22 % 45 – 59 and 4% above 60. The Czech Republic joined the eEurope and eEurope+2003 action plans, which aim to accelerate reform and the modernization of economies in the EU Candidate Countries. The key role in implementing the action plans lies with the Czech Ministry for Telecommunications and Information technology, which is to ensure that 25% of the government agenda is carried out electronically and that at least 50% of the population is computer literate. The Ministry's goal is also to create a more competitive telecommunications environment, give support to e-business, and fulfil the EU candidate countries' initiatives. Several projects are operated by the Ministry and associated bodies under the Action plan for the State Information Policy:

However, the Czech government constantly fails to implement one of the key requests of eEurope plan: cutting the cost of Internet connectivity. Monopolized Czech Telecom is in a strong position to resist any government and regulatory efforts. For instance, the recently introduced ADSL service costs Czech users 42.5 euros (1,363 Kc/$48.03) per month, excluding VAT, for the most-basic level of ADSL service, compared to 19.95 euros in the UK.

The national radio and television council has repeatedly claimed their intention to introduce procedures for regulating the Internet, but with no real outcome. 2001 witnessed a major court case regarding free speech online: P.E.S. Consulting vs Czech Telecom. Czech Telecom was running two Internet portals, Svet Namodro and Quick where they published a series of articles criticising the services offered by P.E.S. Consulting. P.E.S. consulting sued Czech Telecom under the law against unfair competition. The court has ordered Czech Telecom to remove the articles from their server. Czech Telecom followed the order. The articles are however still accessible online, hosted on other servers. Recently, the High Court heard a case of defamation (Criminal Law, Article 206) concerning activity on an Internet discussion forum. The defendant has been found guilty of accusing the pursuant publicly on the Internet forum of bribery and breaking the housing and building law. The High Court confirmed the previous judgement despite the judicial expert analysis that concluded that the authenticity of the post cannot be approved by the terms of the Czech law. The judgement was 150 hours of public service.

It is most likely that other articles of the Criminal Law could be used in a similar way, for instance spreading of drugs (Article 188), child pornography (Article 205) and racism (Articles 198 and 198a). However, nothing has reached the court yet, as the ISP usually removes the content under it's own Terms and Conditions agreement.

A recent and very controversial project financed by the government called "Internet for schools" is based on the "Schools intranet" model, where all the inbound and outbound traffic between the network and the Internet goes through one centralised firewall (Cisco PIX firewall). The project officials claim that the primary – indeed the only - function of this firewall is to prevent from the Denial Of Service type attacks. Nonetheless, the PIX firewall is capable of many kinds of filtering and at the same time each school is being equipped with local filtering software that allows network administrators to block certain sites.

The current law is ambiguous on the question of ISP liability. In brief, the ISP can only be made liable if it is aware of the offending content and it either didn't take any actions to make sure that the content is or is not offensive, or it did so, and failed to remove it. A similar condition applies to the duty to archive log files. A commonly accepted opinion based on the current law status is that the law provides officials with the framework for requesting monitoring and data retention, but only after the court order is received by the ISP.

A few school LAN administrators use various random methods to filter the content. The same is occurring in governmental offices. For example, the Office of the Government of the Czech Republic is using proxy software that is blocking certain web sites. Libraries are mainly free of filtering. Filtering systems are usually set up by individuals (typically school directors with LAN administrators) with no central coordination.

ISP's that provide free dialup access mainly require the CLI (Caller Line identification) enabled to prevent anonymous access. Identification for the use of a computer in a cyber cafe is not required. However, CCTV cameras are widely used in such spaces. The ISP's must give over user information to the police if the police present authority from a judge. The order can only be issued if the criminal proceedings have been initiated and

the defendant knows the charges (160 Article 1 Criminal Law). The only exceptions are urgent and irreversible measures that must precede the criminal proceedings.

There is no bill or act specific to digital copyright. Internet copyright issues fall under the general Copyright Act no. 121/2000. Although the Act has been amended quite recently and introduces several articles relating to digital data such as databases and computer programs and even Internet (spreading of the work via computer networks), the use of this law in a real Internet environment is problematic. The GPL licence for example does not apparently have any legal validity in Czech law. Even downloading free software from the Internet may be considered illegal, as the law requires an explicit agreement obtained directly from the author of the work, while at the same time the validity of online licence agreements faces serious legal problems in the Czech legal system.

Several domains have been removed due to trademark laws. One defendant in 2001 had been running a porn site under the domain wwwpaegas.cz, while www.paegas.cz and Paegas is a well-known name for a major mobile phone operator. The defendant lost on the basis of a law against unfair competition. In the case of quilt.cz (2000) the accuser was a legal owner of the quilt trademark, while the defendant (who was running a very similar type of business in the same region) had registered the domain. The defendant lost the case. In the 2002 case of www.scanservice.cz versus www.scanservis.cz the domain name was phonetically similar to the registered trademark. The defendant lost the case.

Privacy of personal data is protected by the Act no. 101 of 2000 "On Personal Data Protection" The Act regulates the protection of personal data concerning natural persons, the rights and obligations in processing of these data, and specifies the conditions under which personal data may be transferred to other countries. The act also established the Office for Personal Data Protection as an independent oversight body.

Electronic and mail surveillance, wiretapping and interception is regulated under the Criminal Process Law, Article 88. As of the time of writing, no significant changes were made to any laws and regulations in response to September 11th. Police must obtain permission from a judge to conduct a wiretap. The judge can approve an initial order for up to six months. After the six months period the judge can prolong the order. There are special rules for intelligence services. After receiving the order, the ISP or any other telecommunications operators must allow the appointed body (criminal police) to gain remote access to all the user communications data, including access to the electronic mail box, log files, user personal data as well as communication traffic (cell phone locations, dialled numbers etc..).

The law obliges service providers not only to cooperate with the agencies that have the legal right to collect secret information, but also to finance the costs of the monitoring subsystems needed for data collection. However, there is currently no law that would require ISPs to retain users' Internet connection data for a specific time. Nor is there any law that specifies a format of the log files or a means to ensure the data integrity. Nonetheless it would be considered a criminal act if the ISP deliberately deletes relevant data once an order was officially delivered. The telecommunications operators are regulated under Act No. 151/2000 Coll., on Telecommunications.

There are no requirements for ISP's to build surveillance and wiretapping capabilities into their systems, however there are indications that large ISP and mobile and telephone companies are voluntarily and independently building various capabilities that allow them to effectively fulfil the court orders they receive. This is happening in increasing scale with a recent alarming increase of (legal) wiretapping: 341 cases in 2000, 2497 cases in 2001 and 9452 cases in 2002. The numbers do not include wiretapping by the Czech secret service. Many telecommunications operators including ISPs have facilities allowing the police to remotely access individual users' log files. This act does not require a court order (Article 47a 283/1991 and Article 84 of Telecommunications Bill, as opposed to the more rigorous conditions for wiretapping and interception.

There have been cases when poor database security has led to the leaking of customers' sensitive information (even bank details). However, most of this leaked data was not accessible online. There are minor cases when poor security in certain Internet application has resulted in unauthorised access to other users' personal data.

References

Charter of Fundamental Rights & Freedoms 1 http://www.psp.cz/cgi-bin/eng/docs/laws/charter.html?O=3

The 2003 Privacy & Human Rights Report, Electronic Privacy Information Center & Privacy International http://www.privacyinternational.org/survey/phr2003/

Denmark

In general, Danish legislative tendencies, which have traditionally been fairly libertarian, have since 9/11 become more restrictive towards freedom of expression and less protective of privacy.

Technically, 100 percent of the Danish population has free Internet access from public libraries. A recent survey showed that 77 percent have access from home and/or the workplace, 38 percent have broadband access from home (256Kbps or faster) and 64 percent use the Internet at least once a week. Therefore, the digital divide is primarily an issue of access for disabled people.

Under the Danish Constitution, "Everybody is entitled to publish his thoughts in printing, in writing and in speech, responsible however to the Courts. Censorship or any other preventive measure may never again be imposed." However, communication on the Internet in Denmark is liable to the same regulation as other forms of communication, so the provisions in the Criminal Code concerning slander, libel and other offences against personal honour apply to online expression. Unauthorised interference with the privacy of communications is punishable by law. Section 266b criminalises wider dissemination of degrading remarks regarding race, colour, national or ethnic origin, religion, or sexual inclination.

Parliament adopted an anti-terrorism law in 2002 to comply with the UN Security Council's Anti-Terrorism Resolution. The legislation establishes mandatory retention of traffic data by telecommunications and Internet service providers for a period of a year, and gives the police the power under certain conditions to secretly install snooping software on computers. The Ministry of Justice and the Ministry of Science, Technology and Innovation should finish drafting an administrative order regarding ISP data retention in fall 2003. A June 2003 bill aimed at curtailing organised crime further extends these police powers.

In June 2000, the ISP Get2Net announced that it would close down any Web sites hosted on its servers that contained indecent material. After public debate, most Danish ISPs announced that they would not ban legal content for political, religious or other reasons. The recent act implementing the EU directive on Ecommerce, however, creates uncertainty because it says ISPs are neither liable for content on their servers nor mandated to monitor their users' communications. ISPs can, however, be held liable if they are notified of illegal material and fail to take action to remove it. There is therefore some potential for increased censorship if ISPs take down material out of fear of liability. In January 2003, the Danish newspaper Politiken was reported to the police for racist expressions in the chatroom hosted by Politiken Online. Other Danish newspapers have closed down chatrooms to avoid similar situations. In July 2003 to counteract this chilling effect, a committee under the Ministry of Science, Technology and Innovation published guidelines for ISPs.

A few public libraries require both children and adult patrons to use filters. However, most follow the position of the Danish Library Council and the Danish Library Association and adopt local policies and guidelines (net-ethics) to deal with children's exposure to potentially harmful content. There is no ban on content in cybercafés, nor user registration or video surveillance.

The government recently proposed offering all Danish citizens one digital signature for public and private Internet service that would otherwise require a traditional signature. Some civil liberties groups fear this might lead to increased requirements for identification, for instance in chat rooms.

In December 2002 the EU Copyright Directive (EUCD) was implemented in Danish legislation (the Consolidated Act on Copyright). The most radical change was the controversial outlawing of the circumvention of Digital Rights Management (DRM) systems. Distribution or possession (with commercial intent) of technical means whose sole purpose was to circumvent DRM was already illegal. Copyright is not used to directly censor speech on the Internet, but the EUCD implementation has outlawed some forms of expression, and Digital Consumers Denmark has expressed fears over its monopolistic effect on "technical protection measures".

In general, the Consolidated Act on Copyright has not been used to restrict peer-to-peer networks. However, in December 2002, the Antipiracy Group (APG) collected the IP numbers of potential copyright violators (for example, users of KazAa and eDonkey), applied for a court order, acquired the users' names and addresses from their ISPs, and sent out approximately 150 requests for compensation. Civil liberties groups are divided on this issue. In July 2002 a Danish court ruled that the Web site Newsbooster's "deep linking" to articles from Danish newspapers was a violation of both the copyright and marketing practices acts.

The new EU Privacy Directive will force Denmark to allow companies to send advertisements for "similar services" to people that have already

given their address (soft opt-in). This had been banned under the Marketing Practices Act.

Under the Act on Processing of Personal Data (Section 9), citizens have the right to access their own government records. There is no online access to government records. Some public institutions provide records of incoming and outgoing mail from specific institutions/municipalities on their Web sites. The Committee on Citizens' IT rights has recommended improvements to this situation.

References

Digital Rights Denmark
http://www.digitalrights.dk/

The Danish Institute for Human Rights
http://www.humanrights.dk/

The Danish Ministry of Science, Technology and Innovation
http://www.vtu.dk/

The Danish Data Protection Agency
http://www.datatilsynet.dk/

Newsbooster case transcripts
http://www.newsbooster.com/?pg=judge&lan=eng

Big Brother Awards Denmark
http://www.bigbrotherawards.dk/

APC European Internet Rights Project, Country Report — Denmark
http://www.apc.org/english/rights/europe/c_rpt/denmark.html

EPIC and Privacy International, Privacy and Human Rights, Denmark
http://www.privacyinternational.org/survey/

FLA/FAIFE World Report: Libraries and Intellectual Freedom, Denmark
http://www.ifla.org/faife/report/denmark.htm

Wired, Online Hate Has Its Limits
http://www.wired.com/news/politics/0,1283,12996,00.html

France

According to the French Association of Internet Providers (AFA), representing more than 80% of individual Internet subscribers, more than 9 million individual accounts where active in France in March 2003, 20% of them enjoying a high speed connection (either cable or ADSL). This represents 25% of the total number of French households. Nearly 40% of households are equipped with computers. Although this number has grown rapidly, the socio-economic repartition of Internet users does not show the same evolution. A survey published on March 2002 shows that only 42% of the population sample has made a connection to the Internet in the last 6 weeks, from either home, workplace or public access point. When refining this profile, it appears that this Internet user is a man (49%) rather than a woman (36%), under 35 years old (69%) rather than older (29%), preferably working as senior manager (75%) rather than belonging to the working class (36%), living in the Paris area (61%) rather than in rural zones (32%). In summary, France shows a digital divide simply reflecting a social, economic and gender divide.

The French Constitution protects the free communication of ideas and opinions whether expressed through speaking, writing or publishing, but it also states that citizens may be accountable in cases specified by law if these rights are abused. The main provisions against such abuses are specified by the law on Freedom of the press and the law on Freedom of Communication. These laws also generally apply to online expression, condemning slander, libel and other personal offences, as well as hate speech and holocaust denial. While adult pornography material is not illegal, provisions for protection of minor in these laws forbid from exposing minors to such material.

While the right to privacy is not explicitly included in the Constitution, the Constitutional Court ruled in 1994 that it is implicitly protected. The Data Protection Act, enacted in 1978 to protect personal data against abuses by government agencies, is currently being extended by the transposition of the EU Data Protection Directive, a process that should have been completed by October 1998. The Commission Nationale de l'Informatique et des Libertés (CNIL), established by the law of 1978, is the French data protection authority. It receives complaints, issues recommendations, publishes an annual report and is the registrar of all data controllers processing activities. The new law will extend its authority over commercial entities, but will also weaken its control over large government information systems.

The right to access administrative documents is guaranteed by law, and its benefit is mediated through another independent authority, the Commission d'accès aux documents administratifs (CADA), which issues non binding recommendations and annual reports.

Recent legislative process has been challenging these rights. Some provisions have already been enacted, while others are still under discussion. Most of the provisions have been proposed following highly publicised lawsuits against ISPs.

France has commenced the implementation of the EU Electronic Commerce Directive. The draft text of the Digital Economy Law (Loi relative à l'économie numérique or LEN in French) deals with ISP liability, electronic contracts and unsolicited commercial emails, cryptography, cybercrime, and satellite systems. Among them, the most controversial provisions are those concerning cryptography, cybercrime and ISP liability, each of which undermine presumption of innocence and the right to a fair trial, and – additionally - contradicts the French law by allowing self-incrimination. This draft law passed on first reading at both the National Assembly and the Senate. The next readings are expected by the end of 2003.

Providers of cryptography services should provide upon request decryption keys to authorised agents named by the Prime Minister. When a crime or offence is suspected, the public prosecutor or a judge may ask any expert to decrypt data. If the incurred penalty exceeds a two-year prison sentence, military staff may be asked for help. In that case, the decryption method and process would be kept secret, making it very difficult for defence lawyers to question the outcome. The last provision states that anyone having access to decryption keys must provide them. The keys should be provided upon judicial request when cryptography is used for commission, preparation, or facilitation of a suspected crime or offence. Failure to comply with these provisions leads to a jail sentence.

On ISP liability, the draft is a third attempt to introduce a notice and take down procedure in French legislation, although already ruled twice as unconstitutional. Currently, a French ISP can only be held liable for hosting illegal content if it does not obey a judicial order to remove offending content. With the implementation of the Digital Economy Law, ISPs would not be held liable if, after obtaining actual knowledge or becoming aware of facts and circumstances indicating illegal activity, they act expeditiously to remove or to disable access to the information. This would clearly facilitate privatised censorship. In addition, the content hosting definition has been recently

extended by the Senate to include discussion forum hosting.

Moreover, the draft introduces the possibility of ordering French providers to block access to foreign websites. This unprecedented provision would undermine freedom of movement and access on the Internet.

Privacy and data protection rights have already been undermined by two enacted laws. The Daily Safety Law (Loi sur la sécurité quotidienne or LSQ) was adopted on November 15, 2001. The Internal Safety Law (Loi sur la sécurité intérieure, or LSI) was enacted on February 13, 2003.

The September 11th attacks were used as a justification to introduce new provisions immediately before the final adoption of the LSQ, although these provisions have already been proposed by the former government in a previous draft law. ISPs are required to store log files on all their customers' activities for up to one year.

Among the many LSI provisions infringing privacy and other human rights, one authorises the immediate access by Law Enforcement Authorities to the computer data of telecommunications operators, including Internet access providers, as well as those of almost any public or private institute, organisation or company. The second important measure authorises the searching without warrant of any information system, provided that its data are accessible through the network from a computer being searched with a warrant (e.g. all computers in a P2P network may be searched on the basis of a single warrant for one of them). If the data are stored in a computer located in a foreign country, then the access remains subject to applicable international agreements.

These LSI provisions implement parts of Article19 (search and seizure of stored computer data) of the Council of Europe Cybercrime Convention, signed but not yet ratified by France. A ratification law is currently being prepared.

Provisions on ISP liability and on access filtering are the result of extensive lobbying, mainly by rights owner associations and specially major music companies. More recently, during the discussions held by the French government in preparation for the draft law implementing the EU Copyright Directive, the High Council on Literary and Artistic Work Property, or High Council on Copyright (Conseil supérieur de la propriété littéraire et artistique, CSPLA), which includes all representatives of right owners, also advised a 3 year period of mandatory retention of traffic data to trace copyright violations and counterfeiting.

On top of this, intellectual property rights and especially trademark rights have been claimed in several legal cases in order to silence criticisms, e.g. in lawsuits filed against Greenpeace, after the NGO launched campaigns against Esso and Areva, or against the Réseau Voltaire, a French association for Freedom of expression, in a lawsuit filed by Danone group after the association had called for a boycott of its products. All these cases were lost in appeal by the business companies.

In summary, the main change encountered after 9/11 has then been the facilitation of human rights challenges by new laws, with most of the provisions being justified by the fight against terrorism. This situation has – in a way similar to many other countries - weakened the position and actions of human right activists. The reported changes in legislation have succeeded despite important mobilisation efforts from NGOs.

References

IRIS
www.iris.sgdg.org
with comprehensive dossiers on reported legislative processes.

CNIL
www.cnil.fr

CADA
www.cada.fr

Government website dedicated to the Internet
www.internet.gouv.fr

Juriscom
www.juriscom.net, and FDI:
www.foruminternet.org.
Both sites propose most of the Internet jurisprudence decisions.

CSPLA
www.culture.gouv.fr/culture/cspla/conseil.htm

AFA
www.afa-france.com

Survey by IFOP for Tiscali (March 2002)
www.fr.tiscali.com/docs_pdf/2002/IFOPTiscaliFRan%E7aisetadsl.pdf

Germany

The decentralisation of the telecommunications sector and several governmental initiatives such as "Internet für Alle" (Internet for All) has boosted the acceptance and accessibility of the Internet in Germany. As the popularity and importance of the medium grows, so too does the German society's awareness about censorship and data protection issues.

The Telekommunikations-Überwachungsverordnung (TKÜV) (Telecommunication Interception Order), in place since January 2002, mandates the service provider to set up technical and administrative conditions for the interception of telecommunications. Service providers are furthermore instructed to store connection data for future purposes and give the investigative authorities access to that data when requested.

"Projekt Anonymität in Internet" (Project for Anonymity on the Internet - ANON) has been developed and is being run by the University of Dresden (TU) and supported by the German government. The Java Anon Proxy (JAP) application enables anonymous browsing, but this usage is being increasingly threatened as service providers are forced to establish technical and administrative measures to support investigative procedures. These procedures have emerged in response to heightened security as a result of 9/11 and the development of the global campaign against terror. In August 2003 it emerged that ANON was forced by the government to log all access to certain IP address. They had implemented a logging feature which in certain cases broke the anonymity. This requirement was overturned by an appeals court in late August 2003.

At the beginning of 2002, the state of North-Rhine-Westphalia ordered approximately 85 ISPs to block two foreign web pages. Recalling the days when listening to foreign radio stations was prohibited in Germany, civil rights groups, information society organisations and even all internet experts in the Parliament strongly opposed the authorities' decision. They argued that the problem of illegal content publication should not be attacked by restricting user access to the communication infrastructure. While Jürgen Büssow, who was responsible for the blocking order is being awarded with the "Golden Hammer" anti-racism award for the blocking of right wing extremist web content, other users such as Alvar Freude were interrogated by the police for linking to the prohibited web content. His website, odem.org, became a platform for protest action against the blocking order and the links were consequently published as part of the site's coverage of the process. The blocking order led in April 2002 to the first real-life demonstration of the German Internet community in Düsseldorf.

A number of unsolved technical, human rights and data protection issues have emerged around the several cases that ISPs and civil rights groups have brought against the blocking order. The blockage has resulted in user requests to access prohibited content being obstructed or relayed to a third party. At the same time the efficiency of the blockade does not even reach 50% of relevant content. In response to increasing demands for filtering software, University Dortmund, in co-operation with the German companies, Webwasher, Bocatel and Intranet, has tested a filter concept for precise and efficient filtering of web content which would be able to block content from several hundred IP addresses.

This development shows alarming changes in governmental policy. Citizens' rights are becoming increasingly undermined by the monitoring, restriction and even criminalisation of Internet use by bodies in Germany such as the "Datenschutz ist Täterschutz" (data protection is protection of criminals) These initiatives are in contrast to European Parliament policies and even the policy of Die Grünen (the Green Party) currently in power as coalition partner with the ruling social democrats.

References

"Internet für Alle" (Internet for All) – Governmental web site of this initiative
http://www.bundesregierung.de/artikel,-17912/Internet-fuer-alle.htm

"Projekt Anonymität in Internet" (ANON)
http://anon.inf.tu-dresden.de/index_en.html

Erster Teilerfolg fuer AN.ON (27.08.2003)
http://www.datenschutzzentrum.de/material/themen/presse/anonip2.htm

Telekommunikations- Überwachungsverordnung (TKÜV) – Telecommunication Interception Order
PDF download from the web site of the department for economic affairs
http://www.bmwi.de/Redaktion/Inhalte/Downloads/Homepage_2Fdownload_2Ftelekommunikation__post_2FTKUEV-deutsch-englisch1.pdf,templateId=download.pdf

North-Rhine-Westphalia Blocking Order - PDF Download from the web site of the state North-Rhein-Westphalia
http://www.nps-brd.nrw.de/BezRegDdorf/autorenbereich/Dezernat_21/PDF/39sperrverf_022002.pdf

[The order with all URLs included is here: http://odem.org/material/verfuegung/]

"Government Mandated blocking of Foreign Web Content"
A survey on the technical issues of the blocking order done by Maximillian Dornseif.
http://md.hudora.de/

ODEM.org
http://HYPERLINK "http://www.odem.org/"odem.org/
http://censorship.odem.org/

DAVID, a collection of civil rights groups against blocking of websites
http://www.david-gegen-goliath.org/

Chaos Computer Club e.V. (CCC)
https://www.ccc.de/

Förderverein Informationstechnik und Gesellschaft (FITUG e.V.) – Association for Information Technologie and Society
http://www.fitug.de/

Hungary

The Constitution of Hungary contains strong protections of freedom of speech, privacy and access to information. The Hungarian government passed several new security-related laws in 2001, but 9/11 was not the direct cause. Except for some strict, new (and possibly unconstitutional) regulations to block money laundering, these laws were a continuation of earlier legislative practice.

So far, Internet censorship has been limited. In October 2001, the National Security Service (NSS) demanded (without a court order) that a free Web space provider erase a mirror of the NSS's defaced homepage. However, the court pointed out that the right of the NSS to its fair name was uninjured. Both the government and the private sector have some plans for filtering or censoring the Internet.

The national radio and television council (ORTT) published its plan for regulating the Internet in July 2002. The intention is to apply the same rights and liabilities to both offline and online newspapers (that is, requiring emendation on the Internet). ORTT also backed the use of a filtering system to protect minors from harmful content and backed the idea of "notice and takedown" procedures on Internet. However, ORTT said that ISPs providing free Web space should not be responsible for the content of those sites unless the ISP is aware that the laws are being infringed and fails to act. The list of contributors included employees of the Commissioner for Civil Rights, the Commissioner for Data Protection and Freedom of Information, and several NGOs, among them the Hungarian content providers association (MTE).

MTE was founded by the biggest Hungarian content providers in February 2001. In its Code of Ethics, MTE recommends the use of anti-porn filters and asked Internet moderators to erase any vulgar or aggressive postings. MTE wanted to forbid publishing pornography-related materials (whether pictures or text) or publishing anything offensive to good taste in a topic. In December 2002, MTE also warned Hungarian sites not to "deep link" the contents of other pages without permission from the copyright owners.

The Telecommunications Act, adopted on June 12, 2001, obligates service providers not only to cooperate with the agencies that have the legal right to collect secret information, but also to finance the costs of the monitoring subsystems needed for data collection. Providers are required to retain traffic data for six months in the absence of other laws mandating different lengths of time.

The modified Criminal Code (known as the "Hacker Law") was passed in mid-December 2001, and allows for up to a year's imprisonment for accessing a computer without permission. It also prohibits the publication of information or instructions to help in committing computer crimes. Hungary signed the Council of Europe Cybercrime convention in November 2001, but has not ratified it.

References

ORTT
http://www.ortt.hu/index_angol.htm
(English version)

Hungarian Civil Liberties Union
http://www.c3.hu/~hclu/indexuk.htm

NSS
http://www.nbh.hu/english/index.htm
(English version)

MTE
http://www.mte.hu
(no English version available)

Parliamentary Commissioners' Office
http://www.obh.hu

The "Hacker Law"
http://www.complex.hu/kzldat/t0100121.htm/t0100121.htm
(no English version available)

Technology for People Foundation, & Hungarian Big Brother Awards
http://www.hu.bigbrotherawards.org/

Heise, Internet Backdoors in Hungary
http://www.heise.de/tp/english/inhalt/te/12245/1.html

Hungarian Civil Liberties Union (HCLU)
http://www.tasz.hu

eDemocracy
http://www.edemokracia.hu

Italy

Protection of the traditional press from censorship has legally been extended to the Internet (via law 62/2001), forbidding the seizure of a Web site in the same way that it is forbidden to seize a newspaper. However, the Court of Rome refused to recognise this interpretation (even though it has been sustained by the Milan and Latina courts), and allowed the shutting down of a Web site publishing a "personal advertisement" suspected of hiding prostitution activities. The ad was published in the same manner as it would have been in a print newspaper.

The Italian Ministry of Communications engaged as a consultant a Catholic priest who had previously led an anti-child pornography NGO that hired "hackers" to shut down "nasty" Web sites. This has raised strong criticism and concerns from the Italian civil rights movement.

Italian Cybercafes arbitrarily demand passports or photo ID from customers, details of which are recorded alongside logging data, prospectively for use by law enforcement authorities.

The Ministry of Communications also recently took over the Italian Internet Domain Name Authority. It has announced its intention to create a public foundation, expected in May 2003, which will provide domain registration services. Unconfirmed rumours claim that law enforcement bodies may be members of the board or, at least, involved in the foundation.

In 2002, the Italian government made IT security a major priority and it established a National Security Committee (NSC) charged with dealing with all Internet-related matters. The committee members come from academic, military and legal disciplines, and the specific Internet-related skills vary widely among the membership. Civil rights NGOs have been neither involved nor invited to public hearings. The results of NSC activities have not yet been published and it is unknown whether material will be published in the future.

Copyright laws, which already prohibit the independent analysis of security and protection methods used in Italy, and which contain provisions similar to the US DMCA (Digital Millennium Copyright Act) are expected to become more stringent.

In October 2001, the Italian Government enacted Decree No. 374/2001, later confirmed by Law No. 438/2001, as part of its fight against terrorism. The law allows for government agencies in cases involving national security to intercept communications without a court order.

With regard to cybercrime, no court has published official evidence of trials and prosecutions regarding online terrorism or Web site hacking. This is despite the reality that a number of cases have arisen involving child-pornography, lurkers, and copyright infringement. Although a large number of people were involved, no serious evidence has been provided. A serious concern has been raised by the use of computer forensic software based on proprietary licensing to collect and analyse digital evidence to present in court, but this has yet to be considered by the public authorities. Because of the proprietary nature of the software, defence lawyers are unable to carefully check the way the evidence has been handled by law enforcement bodies before trial. Italy is a member of the Council of Europe and has signed the Council of Europe's Cybercrime Convention.

There is a basic absence of input from the several public authorities intended to protect privacy, including the Antitrust Authority, Communications Authority, and Data Protection Commission. The first two were active only in the field of telecommunications voice services. The Data Protection Commission has done little more than issue a generic statement about the need to avoid sacrificing privacy to protect an undefined "public security", and release a position paper about spam, e-mail, and online user profiling. It still has not enacted important, long-awaited measures like the self-regulation of ISPs.

References

International Telecommunications Union statistics report, 2001
http://www.itu.int/ITU-D/ict/statistics/

People online in Italy
http://gandalf.it/data/data3.htm

Andrea Monti, Hacker contro pedofili: crociata o istigazione a delinquere? 3 December 1998
http://www.interlex.it/regole/amonti20.htm

http://www.ictlaw.net/internal.php?sez=art&IdT=1&IdTA=4&IdA=35

ALCEI-EFI - Electronic Frontier Italy "Internet Providers and responsibility in the community legislation"
http://www.alcei.it/english/actions/provider.htm

Russia

The Constitution of the Russian Federation recognises the right to privacy: data protection and secrecy of communications (articles 23, 24), inviolability of the home (article 25), freedom of speech and access to information (article 29). Although there is no widespread practice of Internet censorship, recent events have highlighted the government's attempts to limit these freedoms in order to "protect" the public from "extremists" and "terrorist" forces.

The primacy legislation affecting information technologies including the Internet is the 1995 federal "Law on Information, Informatisation and the Protection of Information", that provides general protection for personal data (articles 11 and 21) and regulates access to information. The law on mass media (adopted in 1991 with numerous additions since then) covers freedom of speech and the media, and bans censorship.

Many issues concerning online censorship, freedom of speech, freedom of information and privacy/data protection are not stipulated in current laws and regulations, and Russia lacks legislation specifically about the Internet. Cases of websites being shut down are rare.

After the hostage drama in Moscow in October 2002 (in which more than 120 people were killed), the Russian Parliament approved amendments to two existing laws on mass media and terrorism. The most important seemed to be the change made to article 15 of the Federal law "On terrorism". This was an attempt to ban all information that "contains expressions that aim at impeding a counter-terrorist operation, advocating and/or justifying resistance to a counter-terrorist operation". This vague definition could include a wide spectrum of materials, for example, interviews with terrorists, anti-war slogans, and the facts relating to human rights violations in Chechnya. These limitations could also be applied to the Internet. The draft was approved by the Senate but it was vetoed by the President.

In October 2002, the Ministry of the Press closed the regional TV station "Moskovia" and said it would close the Web site belonging to the Russian radio station "Echo of Moscow" if the administrator did not remove an interview with Chechen terrorists from the site. The interview was removed, and the Ministry cancelled its request to close the station. In January, Russian hosting provider "Mastak" closed the Web site www.savechechnya.org, which belonged to a Chechen NGO, saying the site was of an "anti-Russian character" and this had caused "problems" for the provider.

In 2002 several Russian private and non-governmental organisations announced that they would begin a joint action against hate speech on the Net. In spite of being promptly attacked by Nazi hackers, the organisers proceeded to close about a dozen racist websites.

Privacy of communications is protected by the 1995 Communications Law, which contains details on telecommunications and the regulation of ISPs. Interference or restrictions such as tapping telephone conversations, scrutinising electronic communications, delaying, inspecting, or seizing postal mail or documenting correspondence, or receiving the information therein are allowed only through a court order. The Law on Operational Investigation Activity that regulates surveillance methods used by secret services also requires a court-issued warrant.

The Federal Security Service (FSB) has conducted phone tapping using the SORM (System of Operative Investigative Activities) system. The next version, SORM-2, requires Internet Service Providers (ISPs) to install surveillance devices and high speed links to local FSB departments which, on issuance of a warrant, would allow the FSB direct access to the communications of Internet users. These rather expensive devices and links are to be paid for by the ISP's themselves. Most ISPs have not publicly resisted the FSB demands to install SORM-2 but the Volgograd-based ISP Bayard-Slaviya Communications has challenged the FSB's demands. The local FSB and Ministry of Communication attempted to have Bayard-Slaviya's licence revoked, but backed off after the ISP challenged their decision in court.

References

J'son&Partners and SpyLOG joint review
http://lawportal.ru/news/news.asp?newsID=2201
(in Russian)

Russian Federation Federal Law No. 24-FZ, 25th January 1995
http://www.datenschutz-berlin.de/gesetze/internat/fen.htm

Gregory Feifer, "Russia: Putin Vetoes Amendments To Law On Mass Media," Radio Liberty web site, 26 November 2002
http://www.rferl.org/nca/features/2002/11/26112002154601.asp

"Putin's gestures to free speech," Index on Censorship, 27 November 2002
http://www.indexonline.org/news/20021127_russia.shtml

"Chechen NGOs reject charge of anti-Russian bias," Radio Free Europe/Radio Liberty, 21 January 2003
http://www.hri.org/news/balkans/rferl/2003/03-01-23.rferl.html#19

"Russia Prepares To Police Internet," The Moscow Times, July 29, 1998.

Moscow Libertarium Forum
http://www.libertarium.ru/libertarium/sorm/

Spain

The key Spanish law governing Internet content is the Ley de Servicios de la Sociedad y la Información y Comercio Electrónico - Society of Information Services and Electronic Commerce Act (LSSICE). This act is the Spanish version of the EU Ecommerce Directive, but is somewhat more ambitious in scope. The Spanish government presented it as the "Internet law" for Spain.

This act gives the government several options for both direct and indirect censorship. Directly, LSSICE makes it possible to shut down a Web site whenever it displays content that threatens basic human rights, including justifications for terrorism or incitement to racism or xenophobia. Indirectly, and more subtly, the act can be applied to almost any Web site in Spain (or the rest of the world) because although it is supposed to apply to only those Web sites that offer commercial services, it includes "displaying of information" as a "commercial service". Therefore, some Spanish activists and lawyers have observed that the ambiguity in the law may be used against a "problematic" Web site. It may be a powerful weapon in hands of the government if it can classify a severely critical Web site as a "commercial service" and fine it up to the law's maximum of €600,000. A small group facing such a big fine would have no choice but to close the site.

The LSSICE includes (in article 36) a provision relating to cryptographic systems that allows for key escrow. This article may be used in the future if the government decideds to implement such a system. Even though key escrow is primarily viewed as a privacy issue, the provision does have censorship implications, as it makes it illegal to use and distribute cryptographic software that evades the key escrow system, and so gives governments a tool for censoring encrypted communications.

A recent change in article 270.3 in the Spanish criminal code makes it a crime to distribute information about how to descramble satellite TV programmes. The web-sinlimite site, among others, was closed down by the computer crime branch of the "Guardia Civil" because it was offering information and/or software to descramble Satellite TV signals. The public prosecutor wanted to use the brand new LSSICE for including links to sites that offer information on how to descrambling Satellite TV signals, following article 17, which establishes legal responsibilities for links to illegal material. The judge, however, decided to dismiss the case against the accused Webmasters of ajoderse.com on the basis that article 17 establishes that a) the person responsible for the link should be aware of the illegal nature of the link and that b) the public prosecutor should present evidence establishing that the links really point to something illegal. The prosecutor was usable to meet either condition.

In May 2003 the Spanish government sued several members of Izquierda Unida (a Spanish left-wing party) as the Webmasters of noalaguerra.org, a Web site dennouncing the Spanish government's position in the recent war against Iraq. The lawsuit is based on the fact that several members of the goverment who supported the decision to participate in the war were called "murderers" and "accomplices of murder". The case has not yet come to court.

The marcianos.net site contains a satirical version of the recent hit "Asereje" by the Spanish band "Las Ketchup", a Flash animation with the song's lyrics changed so as to criticise the government's lack of response when the oil tanker Prestige dropped several tones of fuel along the northestern Spanish coast. The Flash animation also contained fragments of the song's video. Unusually, the SGAE -- the main Spanish association defending musicians' intellectual property rights – threatened a lawsuit if marcianos.net did not either remove the animation, as it contained copyrighted material, or pay a monthly fee to the association as provided by the copyright laws. Several activists suspected this was a government-driven action, suspicions that grew stronger when "Las Ketchup" publicly stated that the band planned no action against marcianos.net and that they thought the use of the song and video was "fair". So far there has been no legal action taken against marcianos.net.

The former state monopoly telephone company Telefonica, on government orders, first denied access to all Spanish users and then blocked the domain www.batasuna.org on the grounds that this site included an "apology for terrorism" and was the site of the political party Herri Batasuna. This is the political branch of the terrorist group ETA and a party that has been recently declared illegal in Spain, also due to its "apology for terrorism".

References

CPSR-Spain
http://www.spain.cpsr.org/

LSSICE (full text in Spanish)
http://www.lssice.com/legislacion/lssice.html

EPIC page on LSSICE
http://www.epic.org/privacy/intl/lssi.html

CPSR-Spain press release about the cryptography law
http://www.spain.cpsr.org/02042003.php

EDRI-GRAMA (CPSR newsletter issue covering cryptography restrictions in Spain)
http://www.edri.org/cgi-bin/index?funktion=view&id=000100000057

Spanish case law about hyperlinks
http://www.edri.org/cgi-bin/index?funktion=view&id=000100000060

Press article in El Mundo about noalaguerra.org
http://www.elmundo.es/elmundo/2003/05/06/espana/1052229102.html

Official press release of the Batasuna webmasters
http://209.210.239.251/ekimenak/zentsura/g_index.htm

Switzerland

Despite Switzerland's relatively advanced Internet infrastructure, there exists a digital divide. According to data collected by the Bundesamt für Statistik the typical Swiss Internet user is young, male, relatively well educated, and relatively affluent,. The main digital divide is between those who are computer-literate and those who are not, a gap that correlates strongly with the level of formal education and therefore also with socio-economic status. In the past few years a public-private partnership has worked to bring computers to public schools, and by spring 2003 almost all public schools had Internet access. However, often this is not used because teachers lack training. In the future this problem may accelerate: the more access to Web sites (and other types of Internet communication) is restricted the more access to information will be limited to those with special technical and social skills.

Switzerland is a signatory to the University Declaration of Human Rights, and articles of its constitution guarantee the right to access information, data protection, and privacy of post and telecommunications, and freedom of speech.

After 9/11, the Swiss government issued an "emergency decree" that has since been extended until the end of 2003 that requires such institutions as hospitals and universities to hand over "suspicious" data to the authorities even in the absence of a formal request. In spring 2003, the government proposed a new law intended to further expand these powers.

The Parliament approved a new law on interception of communications in 2001. The law requires ISPs to retain communications data for six months. In the case of mobile phones, such data includes location data, requiring mobile network operators to constantly track phones and store the data they so collect. The law also requires ISPs to have the capability of interception email in real time. In case of an interception order, the ISP must forward a copy of every email belonging to the targeted individual to a special police service in Berne. Lobbying organisations like the SIUG, as well as consumer organisations and data protection officers, regularly stress that email and Internet traffic are not anonymous at all except when using encryption programs like PGP. The SIUG and Big Brother Awards Switzerland are organising workshops on "safe surfing". Cryptography is not restricted in Switzerland. In Spring 2003, the Swiss Parliament decided to require compulsory registration for all users of prepaid mobile phone calling cards. It is, however, illegal to monitor Internet traffic in enterprises.

Switzerland signed the Cybercrime Convention in November 2001. A federal coordination unit for cybercrime control (KOBIK), was formed in February 2002 and became operational in April 2003. The agency's mission is to look for "illegal content" on the Internet and to prepare prosecutions. Individuals may report crimes, including hacking and pornography, to the unit.

The Criminal Code prohibits the posting of illegal materials such as racist speech and online incitement to violence. The question of ISPs' liability for content hosted on their servers is not clear and there have been no court cases. However, in several instances the federal police have issued advice to ISPs to delete or block access to specific Web sites. For example, the examining magistrate of the Canton of Vaud asked ISPs to manipulate the DNS to block access to specific Web sites, and there have been cases where a big company tried to block employee access to the site belonging to a union. The big commercial ISPs especially have tended to honour requests to block or delete sites, and they have added paragraphs to their Acceptable Use Policies to the effect that they may delete Web sites or accounts without the client's consent. Legally, it seems that ISPs can be made liable if they continue to host Web sites with illegal content after being made aware of them. However, ISPs are not required to proactively check the content of the Web sites they host. Some commercial enterprises use filtering software, but these are not used by public institutions.

There have been no court cases involving the use of copyright law to limit speech on the Internet. However, in November 2001 Microsoft Switzerland sent a letter to many companies asking them to hand over detailed data on all PCs and software in use. There were protests over this letter, mainly by the Union Syndikat (www.syndikat.ch).

References

Union of online workers
http://www.syndikat.ch/

Swiss Network Operators Group (Swinog) homepage
http://www.swinog.ch/

2001 Wiretap law
http://www.admin.ch/ch/f/rs/c780_1.html

Laws on interception of telecommunications traffic and email
http://cryptome.org/ch-ilets-regs.htm

Criminal Code (Schweizerisches Strafgesetzbuch)
21 December 1937, (revised 1998)
http://www.admin.ch/ch/d/sr/c311_0.html

Disposal by the Canton Vaud (unofficial copy, french)
http://www.nrg4u.com:80/abuse/canton-de-vaud.pdf

Coordination Unit for Cybercrime Control (CYCOS)
http://www.cybercrime.admin.ch/e/index.htm

Swiss Council of Press Guidelines,
http://www.presserat.ch/14280.htm

Federal Office of Justice
http://www.ofj.admin.ch/

Federal Data Protection Commissioner
http://www.edsb.ch/e/aktuell/index.htm

http://www.isps.ch

Turkey

The Turkish government took a hands-off approach to regulation of the Internet until about 2001. At that point, the Turkish government introduced a parliamentary bill with the intention of regulating Internet publications according to the same rules that governed the mass media. There were strong protests and the bill was vetoed by President Ahmet Necdet Sezer, in June 2001. Sezer at the time stated that:

> *"The most important aspect of Internet broadcasting, which is like a revolution in communication technology, is that it is the most effective area for freely expressing and spreading ideas and for forming original opinions… Leaving the regulation of the Internet to public authorities completely and linking it to the Press Law does not fit with the characteristics of Internet broadcasting."*

However, in May 2002, the Parliament approved the Supreme Board of Radio and Television (RTUK) Bill (No 4676). The bill regulates the establishment and broadcasting principles of private radio and television stations and amends the current Turkish Press Code. It includes provisions that would subject the Internet to restrictive press legislation in Turkey. Although it tries to apply only some aspects of the Press Code (such as those to do with publishing "lies"), vague provisions are open to various interpretations. The rationale behind these provisions is the silencing of the criticism of the Members of the Turkish Parliament and to silence political speech and dissent. It should be noted, however, that no action has been taken in relation to any Web publications under the provisions of the legislation.

Apart from this widely discussed and protested legislation, the only notable Internet related regulation exists in relation to cybercafes in Turkey. The regulation is mainly concerned with location (for example, cafes may not open near schools) and requires cafes to be licensed, like gaming places. Minors under the age of 15 are not allowed into cybercafes, and access to illegal sites (such as those that contain obscenity or affect national security) or allowing minors access to pornography is prohibited. The regulations do not specify, however, whether the cafes need filtering software or how they should achieve blocking.

There are also a handful of cases involving Internet-related prosecutions and attempts at censorship involving the Turkish criminal code. So far, these remain as atypical cases and the prosecutions of both Emre Ersoz and Coskun Ak under section 159 of the Turkish criminal code haves been heavily criticised.

Coskun Ak, a former moderator of the forums operated by Superonline, one of the largest ISPs in Turkey was sentenced to four years in prison for insulting and weakening the Republic of Turkey, the Military Forces, the Security Forces, and the Ministry of Justice for a message posted by an anonymous reader. It was later reduced to 10 months for each insult (40 months total) after the good conduct of the accused in court was taken into account. On 14 November 2001, the Supreme Court reversed this ruling and decided that Ak's case should be reconsidered once experts selected from universities look at the situation: and "... investigate the responsibilities of Superonline (as an ISP), where Ak worked at the date of the crime ... whether it can be regarded as a content provider and the exact position of Ak in the company ..." On retrial in early 2002, the 40 months' imprisonment was commuted to a fine of TL 6 million (app. $4). On 24 April, 2003, this second sentence was quashed by the Court of Appeal.

In an earlier incident Emre Ersoz, 18, received a ten-month suspended sentence for "publicly insulting state security forces" after comments he made in an online forum operated by one of Turkey's ISPs. Insulting state authorities and the police is a criminal offence in Turkey, under section 159(1) of the national criminal code. Ersoz, in a debate over allegations of rough police treatment of a group of blind protesters complaining about potholes in the nation's capital, Ankara, said he believed that the national police had beaten the protesters. Ersoz then repeated the allegation in a current events forum provided by the ISP Turknet. In fact, Ersoz was mistaken: the protesters had been beaten by municipal officers, not by the national police whom he specifically criticised in his posting.

Ersoz, who signed off using his real name and e-mail address, was reported to authorities by another person on the Turknet forum. State prosecutors then asked Turknet for Ersoz' full address, and the ISP complied. At 3:30 a.m., Ersoz' home was raided by a special anti-terrorism police squad, and he was taken into custody and held by police for two days. The public prosecutor of the Beyogly municipality in Istanbul brought the charges and demanded a sentence of one to four years. Ersoz pleaded not guilty, claiming his writings were not in the public domain because the forum was open only to Internet users. Ersoz' ten-month sentence was suspended on the condition that he not be convicted of similar charges during the next five years.

As of mid 2003, Turkey has not signed or ratified the COE Cybercrime Convention nor the additional first Hate Speech protocol of the CyberCrime Convention. But it remains to be seen what

approach will be adopted by the new Turkish government. A draft freedom of information bill has been released for consultation, and Turkish government continues to follow the Turkish National Programme for the Adoption of the Acquis in order to join the European Union, which requires speech-related restrictions to be relaxed according to the criteria in Article 10 of the ECHR.

References

Altintas, K., Aydin, T., Akman, V., "Censoring the Internet: The Situation in Turkey," First Monday, May 2002
http://www.firstmonday.dk/issues/issue7_6/altinta/

Presidential Statement in relation to proposal to amend the Press Law, 18 June, 2001
http://www.cankaya.gov.tr/ACIKLAMALAR/18.06.2001-1159.html

Statement by Dr. Yaman Akdeniz in relation to the Internet related provisions of the Turkish Supreme Board of Radio and Television (RTUK) Bill (No 4676), 15 May, 2002
http://www.cyber-rights.org/press/tr_rtuk.htm

http://www.birlik.com/english.htm

Akdeniz, Y., "Turkish teen convicted for Web postings," Freedom Forum, 08 June, 1998
http://www.freedomforum.org/templates/document.asp?documentID=11277

EU Report on Turkey
http://europa.eu.int/comm/enlargement/turkey/pdf/npaa_full.pdf

Ukraine

According to the Information Society Foundation of Ukraine there has been an increase in the number of Ukrainian Internet users over the last four years by as much as 70% annually. By the end of 2002 there were 2.5 million users (5.2% of total population) and 1 million of them were regular visitors to the Internet. Up to 80% of the users live in seven regional centers.

The freedom of speech is one of the most vulnerable rights in Ukraine. The traditional media such as TV and broadcasting in most cases depend on the official pro-presidential propaganda. One of the visual proofs of political censorship in Ukraine is the practice of temniki (guidelines for the content of news reporting) distribution among the top managers of national television stations and newspapers by the Presidential Administration. The censorship effectively denies access to objective information for the majority of the Ukrainian citizens.

The national domain ".ua" was registered in December 1992 but the first Ukrainian media appeared on-line only in 1999. Since then, electronic media activity in Ukraine has created a significant impact on the success of the struggle for democracy, as e-media is the only independent media in the country. Nevertheless the significant increase of popularity of the Ukrainian e-media does not rival television, as this is still the most widely utilized form of mass media.

There is a lack of understanding among the majority of Ukrainian policy makers about the nature of the Internet as a global medium. This situation explains in part the unqualified interventions and efforts to control the Internet by implementation of legal restrictions. The official position of President Kuchma towards Internet freedoms is negative.

In June 2001 at the Summit of Central European heads of states in Verbania, Italy, President Kuchma delivered a speech stating that freedom of speech on the Internet results in the "dissemination by certain European websites of ultra-national propaganda, instructions for terrorists, pornography and other things of such kind" constituting "the direct threats to the democracy, people and peoples, and moral health of nation."

The chief of Security Service Yuri Radchenko said on July 14, 2001 that the SBU "has no plans to control the Internet in Ukraine but rather it would like to register all users of Internet in Ukraine." In December 2001, the government adopted the Decision of the Council of National Security and Defence of Ukraine enacted by the Ukase of President on "The Measures for the Improvement of National Information Policy and Safeguards of Information Security" of Ukraine of December 6, 2001 (No. 1193/2001). The Ukase obliges the Cabinet of Ministers to elaborate and introduce draft laws creating an obligation on Internet providers and e-media to apply for licenses. Laws will also mandate the monitoring of Internet-traffic and storage of Internet-traffic data for six months. The Cabinet of Ministers has not yet submitted the bills to the Parliament. A previous attempt to do so was rejected by the Parliament in 1999.

The idea to consider the Internet as a form of mass-media and to treat online editions in the same way as digitally-printed press is widespread not only among Ukrainian officials but representatives of e-media as well. Oficials would like to register e-media in order to gain some device of influence; e-media would like to do so in order to obtain the rights and privileges of the offline press which is provided by the legislation in force. This includes provisions for professional and social rights for journalists.

Such issues were actively discussed by policy makers in 2001 with regard to the idea of public registration of e-mass media. The grounds for it resided in the Article 1 of the Statute on Printed Mass Communication Media (Press) in Ukraine of November 16, 1992.

Fortunately no serous attempts have been made to force e-mass media to register so far, but the regulatory situation is vulnerable. The uncertainty of the legal status of e-media in Ukraine caused an incident when the representatives of the on-line newspaper "Ukraiynska Pravda" were refused accreditation by the General Prosecutor Office on December 5, 2002

The legislation in Ukraine foresees the liability of printed mass-media (press) for the publishing of defamatory material. The Internet is not considered by the courts as the printed source of information and offline reprinting of online defamatory information thus constitutes a violation of the law. The majority of Ukrainian e-media journalists would like to have the same rights as their colleagues working for the offline press. But they do not wish to be liable for on-line defamation. Such dilemmas of e-media legal status and liability for on-line defamation were used as formal ground for the act of self-censorship.

Recognising these problems, the members of the Committee on Journalist's Ethics (an independent professional body) drafted the Declaration on a Clear Internet. The representatives of the most

popular Ukrainian e-media discussed the draft at the workshop organized by the CJE on January 29, 2002 and rejected it.

It is likely that amendments to the legislation aimed at giving the journalists of e-media the same professional and socials rights are to be introduced in the Parliament soon.

Following Parliamentary hearings on "Society, Mass Media, Authority: Freedom of Speech and Censorship in Ukraine" held on December 12, 2002, the Statute on Amendments to Several Laws was adopted on April 3, 2003 by 252 votes of the members of Parliament. The Amendment clarifies the term "censorship", facilitates the access to the information held by public bodies, and limits the possibilities of suppression of mass-media through the device of court penalties arising from defamation action.

Even in the absence of legislation, there have been numerous assaults against electronic media. In June 2001 the private apartment of Mr. Yeltsov, the editor-in-chief of e-media "Ukraina Kriminalna" (Criminal Ukraine) was searched by the SBU. This action took place following the on-line publication of secret documents and an article titled "From the Life of Derkatch's Family" on the activity of former chief of SBU Leonid Derkatch and his son, a member of Ukrainian Parliament, which described their business relations with Ukraine's oligarchy.

In February 2002 the premises of the on-line political newspaper "Obkom" were searched and computer equipment and archives were seized by tax administration officials even though they only had a warrant to search a bank located on the floor below. Although the tax authority said later the search had been done "by accident," the computers were never returned. The on-line publication recommenced nearly a year after the incident. The Kyiv City Regional Prosecutor Office refused to initiate criminal proceedings against officials due to the "lack of legal grounds".

In October 2002 the editorial premises of the on-line newspaper of the Regional Department of the Ministry of Internal Affairs "Antiterror" (Lviv City) was searched and PCs were seized by police because it had published the text of the indictment against President Kuchma issued by the judge of the Kyiv Appeal Court. The contracts with all editorial staff were terminated a few days later.

References

E-Ukraine: report, Version 5.0 (February 4, 2003) of the report of the Information Society of Ukraine Foundation
www.isu.org.ua

Negotiating the News: Informal State Censorship of Ukrainian Television. - Human Rights Watch. - March 2003, Vol. 15, No. 2 (D)
www.hrw.org/reports/2003/ukraine0303/

Information Policy of Ukraine: Access, Transparency, E-governance' at
http://www.internetrights.org.ua/index.php?page=news&date=2003-08-09

UNIAN, January 8, 2003
www.unian.net/ukr/news/news-31369.html

The list of regulations on the activity of mass-media in Ukraine is available at
en.imi.org.ua/elements/law.shtml

Translation of the Institute of Mass Information
en.imi.org.ua/articles/1023209329668/

Article 19 Pages on the Ukraine
http://www.article19.org.ua/indexe.html

Article XIX, Statement on the draft Law of Ukraine on the Insertion of Changes to Certain Laws of Ukraine as a Result of the Parliamentary Hearings "Society, Mass Media, Authorities: Freedom of Expression and Censorship in Ukraine", April 2003
http://www.article19.org.ua/laws/april2003e.html

United Kingdom

According to the telecoms regulator, Oftel, more than 60 percent of British adults have used the Internet at some time in their lives and more than 50 percent of households are online. Only 9.3 percent of Internet subscribers have ADSL or cable broadband (January 2003, up from 8.5 percent in October 2002), but the number is growing rapidly now that prices have dropped and the monopoly ADSL wholesaler, British Telecom, has become more aggressive about rolling out its service. The top five ISPs - AOL, BTOpenworld, Freeserve, Ntl, and Tiscali - more or less equally share 80 percent of the Internet access market.

Outside of the US itself, the UK was hardest hit by the September 11 attacks, and many measures to increase surveillance and law enforcement powers were introduced. Many of these were not new, but reintroductions and extensions of legislation and ideas that had been rejected by the public in the 1990s or codes of practice related to existing bills whose supporting regulations had not yet been published. Key pieces of legislation include the Regulation of Investigatory Powers Act (RIPA, 2000), the Anti-Terrorism, Crime, and Security Act (ATCSA, December 2001), and proposals to create a new national "entitlement card", in effect, a national ID card (under consultation in 2003).

In December 2001, the Parliament approved the Anti-terrorism, Crime and Security Act (ATCSA). The law allows the Home Secretary to issue a code of practice requiring communications providers to retain users communications data (but not the contents of their emails) for the purpose of protecting national security. It only applies to data that is already being held by the telecommunications providers for business purposes.

This was the culmination of several years of effort to adopt data retention into law. A leaked submission by the police and intelligence services to the Home Office in 2000 proposed a seven year data retention scheme. The Home Office began a consultation in 2003 on voluntary retention of data by communications providers and is considering the responses.

ISPs have resisted these demands on the grounds of cost, and the Information Commissioner has obtained a legal opinion that the ATCS requirements would create a disproportionate invasion of privacy under the Human Rights Act 1998 because of the wide range of reasons for access to that data under RIPA. A review by the Parliament's All Party Internet Group estimated that over one million requests a year are made for communications data, mostly the names and addresses of users. Discussion is continuing between the government and ISPs, who favour a policy that would require ISPs to retain only the data of a particular individual under court-ordered surveillance.

The Regulation of Investigatory Powers Act regulating interceptions of communications became law in July 2000. Many legal experts, including the Information Commissioner, believe that many of the provisions of the Act violate the European Convention on Human Rights.

The RIPA authorises the Home Secretary (rather than an independent court) to issue warrants for the interception of communications and requires Communications Service Providers to provide a "reasonable interception capability" in their networks. Telephone taps for national security purposes are authorised by the Foreign Minister.

Public authorities designated by the Home Secretary can access "communications data" without a warrant. This data includes the source, destination and type of any communication, such as mobile phone location information and web browsing logs (but the full URL is considered content subject to a warrant). In June 2002, the Home Office announced that the list of government agencies allowed under the act to intercept web traffic and mobile location information without a warrant was being extended to over 1,000 different government departments including local authorities, health, environmental, trade and many other agencies. This caused a substantial controversy, especially after the Surveillance Commissioner even before the proposed expansion admitted in his annual report that "I clearly cannot carry out meaningful oversight of so many bodies without assistance". Home Secretary David Blunkett announced a few weeks later that he had "blundered" and withdrew the order. A public consultation on access to communications data was held in early 2003 and the Home Office is at the time of writing reviewing the responses.

RIPA also allows senior members of the civilian and military police, Customs, and members of the judiciary to force users to hand over the plaintext of encrypted material, or in certain circumstances decryption keys themselves. This section has not yet been implemented.

The Department of Trade and Industry is currently holding a consultation to implement the 2002 EU Directive on privacy and electronic communications. The regulations will place new rules on cookies limit Email and SMS spam. The DTI plans to have the regulations come into force on 31 October 2003.

In July 2002 the government launched proposals for a national "entitlement card". The card would not be compulsory to carry, but would be needed to gain access to state benefits such as national insurance, education and health, as well as legal employment and financial services. In mid 2003, Home Secretary David Blunkett endorsed a biometric-enhanced smart card. Shortly afterwards, however, Prime Minister Tony Blair indicated that the cards present huge logistical and cost issues. It is likely that the card will be formally proposed in the fall.

Internet censorship is generally limited. The question of ISPs' liability for content hosted on their servers is an ongoing issue. In 1999, Laurence Godfrey sued leading ISP Demon Internet for defamation when the service failed to remove a Usenet posting, forged to appear as if it came from Godfrey, from its servers after a faxed request. The case was settled out of court and Demon paid Godfrey £15,000 plus legal costs. The case established that ISPs were required to have notice-and-takedown procedures in place for taking down disputed material.

The Law Commission in December 2002 released a report on "Defamation and the Internet". The Law Commission found that " the current law places secondary publishers under some pressure to remove material without considering whether it is in the public interest, or whether it is true. These pressures appear to bear particularly harshly on ISPs, whom claimants often see as 'tactical targets' " and discussed means of limiting this liability.

The Internet Watch Foundation, an independent organisation that was created in 1996 and endorsed by government and law enforcement agencies, operates a hotline to which members of the public can report questionable material they find online. The IWF reviews the material and if it is illegal under UK laws such as the Obscene Publications Act 1959, the Protection of Children Act 1978, or the Public Order Act 1986 (this applies primarily to hate and racist speech), reports the material to police and advises British ISPs to remove it from their servers. The material so removed is thought to be primarily child pornography.

Proposals for implementing the EU Copyright Directive were published in 2002, but elements such as criminalising circumvention technologies and the lack of protection for cryptographic researchers were so widely protested that the law itself was delayed until 2003. So far no new proposals have emerged.

References

Privacy International UK Privacy Pages
http://www.privacyinternational.org/countries/uk/

Cyber-Rights & Cyber-Liberties
http://www.cyber-rights.org

Regulation of Investigatory Powers Act
http://www.hmso.gov.uk/acts/acts2000/20000023.htm

Anti-Terrorism, Crime, and Security Act
http://www.hmso.gov.uk/acts/acts2001/20010024.htm

Internet Watch Foundation
http://www.iwf.org.uk

ISPs reject voluntary data retention
http://www.guardian.co.uk/internetnews/story/0,7369,816523,00.html

NCIS submission on communications data retention
http://cryptome.org/ncis-carnivore.htm

Law Commission, Defamation and the Internet - A Preliminary Investigation, Scoping Study No 2 December 2002.
http://www.officialspin.com/documents/pdf/defamation2.pdf

Uzbekistan

Civil rights are limited in Uzbekistan. The Constitution provides for a presidential system with separation of powers between the executive, legislative, and judicial branches. The next presidential election is due in 2004. In practice, however, power resides in the executive branch. Since the 9/11 attacks, Uzbekistan, because of its proximity to Afghanistan, has hosted US airbases in return for increased aid from the US. The US has been criticised for not using this partnership to press for human rights improvements within the country.

Uzbekistan's population of Internet users doubled in 2002 from the 139,000 reported at the end of 2001. According to the Uzbekistan National News Agency, 73 percent of these users are located in the capital, Tashkent. Most users in the region depend on Internet cafes for access; there are more than 100 of these operating in Tashkent, with just one each in the other major regions of Uzbekistan, Karakalpakistan and the Srukhandarya Oblast.

Internet access became available in the country in the mid 1990s, quickly followed by reports that Uzbekistan exercised a great deal of control over access. These reports were confirmed in early 2003 when ISPs were unofficially told to block access to the centrasia.ru Web site, where a series of four controversial articles was first posted (they were later copied to other Russian sites). These were attributed to "Usman Khaknazarov" and alleged that President Islam Karimov, in power since 1991, and his aides were all involved in corruption, and encouraged Uzbeks to unite to oust Karimov's government. Because public access to information about the government is so limited, these articles were taken very seriously and read widely; people with Internet access made dozens of copies for friends and relatives. Many believed the allegations. The identity of "Usman Khaknazarov" remains hidden, although the articles contain details that could only be known by those in power. Internal inconsistencies suggest, however, that more than one author may be involved. No one has been arrested for putting up the websites, since these are all hosted in Russia or in Western countries.

A number of other sites were also blocked, along with uzbekistanerk.org and birlik.net, the Web sites belonging to the opposition parties. In total, nearly a dozen popular Web resources remain inaccessible. The blocking was denied by Uzbek officials, but access to these sites is only possible via the Web's anonymised browsing services, of which the most popular in Tashkent are anonymouse.ws and Webwarper. However, only advanced Internet users are aware of these free services. Meanwhile, state-controlled television broadcast a series of pro-Karimov programmes.

The news media are tightly controlled by the government, there are no independent news outlets (according to Human Rights Watch) and freedom of speech is limited, even though the Constitution expressly prohibits censorship of the press. In July 2003 an independent journalist who leads a group focusing on media freedom, Rusian Sharipov, was arrested on charges of sex with minors and managing prostitutes. He claimed his prosecution was directly linked to his journalistic activities. Sharipov is also openly gay, while Uzbekistan has not liberalised the laws against sex between men since the Soviet era.

A new law "Principles and Guarantees of Freedom of Information" went into force in February 2003. It provides for access to information but also requires the "[e]stablishment of systems of resisting informational expansion, prevention of the use of informational systems aimed at deforming the national consciousness and distancing the community from its historical and cultural traditions and customs" and the stopping of information in the name of "Protecting social and political stability, inter-ethnic and inter-denomination accord as well as protection of the community's moral and spiritual principles."

References

Union of Independent Journalists of Uzbekistan
http://www.uiju.org/internet.html

Coordination Council for Development of Computerization and Information Communication Technology
http://www.ictcouncil.gov.uz/english/news.html

Human Rights Society of Uzbekistan "Civil Support"
http://pougs.boom.ru/news.html

EurasiaNet
http://www.eurasianet.org/resource/uzbekistan/articles/index.shtml

UZ Report
http://www.uzreport.com/eng/index.cfm

Internews Uzbekistan
http://www.internews.uz/

Draft Law, Principles and Guarantees of Freedom of Information
http://www.privacyinternational.org/countries/uzbekistan/foi-draft-02.doc

ARTICLE XIX analysis of the draft Uzbek FOI law
http://www.article19.org/docimages/1504.doc

Resolution of Cabinet of Ministers of the Republic of Uzbekistan On decentralization of access to international computer networks, No 352, October 10, 2002
http://www.ictcouncil.gov.uz/english/post352.html

Uzbek Internet something of an anomaly, Moscow Times, October 2001
http://www.uzland.uz/2001/october/29/10.htm

Uzbekistan: Internet Usage Up, But Controversial Websites Blocked, RFE/RL, January 2003
http://www.rferl.org/nca/features/2003/01/31012003182158.asp

Internet Censorship in Latin America
Regional report

Legal issues
An overview[1] of the different constitutions in Latin America shows that there are constitutional protections in place for: Freedom of speech, Access to information and Privacy of data and communications in most countries in the region.

The Pact of San Jose of Costa Rica, officially known as the "American Convention on Human Rights" (ACHR) has been ratified by most of the Latin American countries[2]. Article 13 of the ACHR contains some rules pertaining to censorship. These countries are also subject to the jurisdiction of the Inter-American Court of Human Rights, a body that has rendered many decisions in favor of the right to freedom of expression. Furthermore, the Inter-American Commission on Human Rights has appointed a Special Rapporteur for Freedom of Expression who provides legal assistance on freedom of expression and produces an annual report on the state of this right in America[3].

> "Internet censorship has not become a major issue in Latin America"

These provisions, together with the existence of a Human Rights Court at the international level provide strong safeguards for freedom of expression in Latin America[4].

Laws and regulations that may impact online privacy and free speech.
Laws and regulations in Latin America are broadly drafted, and therefore easily applied and interpreted to encompass new technologies. Civil law countries tend to interpret statutes in a more open fashion that common law countries and for the civil law judge it is mandatory to find a legal solution to a case applying traditional laws by analogy (except for criminal cases). That is why a few years ago a legal report stated that: "Internet censorship has not become a major issue in Latin America"[5].

There are basically no specific restrictions over use of the Internet in any of the surveyed countries, except for Mexico where there is a specific requirement for pornographic material filtering devices. In Brazil, there are no specific requirements for filtering devices, but rather it is necessary to post notices in web sites that contain pornographic material. And in Chile the Congress has already expressed an interest in trying to limit immoral content and pornographic content information transmitted via Internet but the bill was never approved[6].

> "As far as the research has shown, there are no websites within Latin America that have been banned or 'taken down' due to political or religious reasons."

In the last years, however, there are some content restrictions for Internet in many of the surveyed countries: Argentina, Colombia and Peru have enacted specific statutes that aim to curtail pornographic material with filtering software or devices in public access places (mandatory) or personal home computer (voluntarily for each user, in the case of Argentina).

In Latin America wiretapping requires an order from a judge. This requirement is found either in the Constitution of the criminal procedure laws (see law 23.984 in Argentina; law 9296/1996 in Brazil; law 19.423 and law 18.314 in Chile). Specially after September 11, 2001, in Argentina the Federal Congress enacted the Intelligence Law (Law 25.520, Fed. Reg. Nov. 27. 2001). The law forbids any intelligence agency to collect personal data from individuals or companies without a judge's order (section 4) and provides for the privacy of telecommunications of any kind including Internet messages (section 5).

Speech issues
As far as the research has shown, there are no websites within Latin America that have been banned or 'taken down' due to political or religious reasons. Only one libel case in Costa Rica led to a judicial order removing the name of the plaintiff from the web site of the newspaper La Nacion[7]. The judgment ordered that the links between the last name of the plaintiff and the impugned articles be removed from the electronic version of the paper La Nacion and that a link be established between these and the contentious part of the sentence. The case was taken to the Inter American Court of Human Rights. On September 7, 2001 the Court granted provisional measures against the State of Costa Rica in favor of the two sentenced journalists. The Court also requested that the state suspend the order of publication in La Nacion of the part of the judgment of the Criminal Tribunal of San Jose that declared guilty the journalist, as well as

the order requiring the link, in the Internet version of La Nacion, between the articles cited in the complaint and judgement[8].

There is an Anti-discrimination law in Argentina that bans hate speech. However, some authors doubt that this law may be constitutionally upheld if it is applied in a generic way[9].

> **"Many countries are developing plans to increase Internet presence and access to electronic resources."**

The Criminal Federal Court of Appeals of San Martin, Province of Buenos Aires, has ruled that the sale of Nazi literature and objects on the Yahoo! auction site was not a crime punishable under the Argentine Anti-discrimination Law.

In Chile, a parliamentary motion has been submitted in the Chamber of Deputies that aims at censoring the contents of the Internet[10]. The bill proposes to punish individuals that use the Net to disseminate content that is offensive to morals, public order or "proper customs." This kind of description of conduct is known as a "blank penal law," because the determination of whether a given conduct is contrary to the law is in the hands of the judge. It is in his judgment to decide if a given behavior is against what is understood to be "morally correct," or if it belongs to the realm of the private, and therefore outside of the interest of the general community. It is also the judge who determines if something is against "proper customs." Commentators argued that because of the territorial nature of the law, this bill is little else than a romantic declaration of intentions. It would only carry force within the boundaries of the Republic of Chile, and this makes it patently useless, as the Internet is by nature independent of political boundaries. The only way the law could apply would be if the server that hosts a given content is in the territory of Chile. This is the law's Achilles' heel; a weakness that can easily be exploited to circumvent it. A notorious example of this is the case of the book called "The Black Book of Chilean Justice." Because of a ban on the sale and reproduction of this book, a result of a suit brought by a Supreme Court judge who appeared prominently in the book, the courts ordered all copies of the book to be confiscated. The whole country was left wondering about what was in the book. But everyone soon learned everything when the whole contents of the book were made available over the Internet, in a server physically located abroad. A perhaps nontrivial detail was that the domain name of this server was a ".com" and not a ".cl", which placed it even further from the reach of Chilean law.

The rest of the articles of the bill are programmatic and the text is vague in many respects. However, this kind of law would not only be ineffective, because of the limitations of territorial law when faced with the ubiquity of the Internet, it is also unnecessary. The legal system already contains laws that allow the prosecution of violations of personal reputation, and of behaviours that are against public morals and public order, such as the Law of Abuses of Publicity (Nº 16.643) and the Penal Code. However, the right to freedom of information without prior censorship is guaranteed by the Chilean constitution, in its article 19 Nº 12; and the implementation of this guarantee and its limitations due to civil and penal responsibility that arise from the exercise of this freedom are also mentioned in the law.

Other laws may restrict another kind of content. For example, on July 30, 2003, the Brazilian House of Representatives approved Bill of Law No. 5.460/01 which would criminalise sexual images involving minors on the Internet, in magazines or any other visual media. This Bill would expand the Brazilian Minors Statute (Law No. 8,069/90), which only criminalises sexual images of minors on television, cinema or theatre. In addition, it would enlarge the scope of who may be prosecuted as well as impose an increased penalty of 2 to 6 years imprisonment plus fine. The Bill will now be submitted to the Brazilian Senate[11].

Anonymity on the Internet.

The Constitution of Brazil bans anonymity (see section 5.IV). The Constitution of Venezuela of 1999, after establishing freedom of expression provides that "anonymity is not allowed" (section 57). There is no mention of anonymity in other Constitutions. In Bolivia anonymity is recognised by the law of press (section 8) and it is a crime to reveal information related to anonymity (section 9).

In Argentina, a bill was introduced by Rep. Norma Godoy (see TP 5371-D-01) in the year 2001 to regulate the use of fax and Internet communications from public places. The bill would require places like cybercafes and public call centres to establish a registry of users (collecting personal such data as name, national id, and time of the connection). They may be required to keep a log book that must be presented to the authorities upon request. Violation of these laws would result in imposition of a fine or closure of the shop. The bill was never discussed in Congress.

Another bill wants ISP's to carry and store traffic data (see next point).

Status of ISPs who host content for their clients. Liability in terms of the law for the actions of their users.

There is no clear law in Latin America dealing with the liability of Internet service providers. However, many authors argued that strict liability may be applied to content published in web sites.

A judicial decision in Chile from a court of appeal established that any dispute related to content displayed on the Internet must be resolved according to the Constitution and in compliance with general provisions regarding civil and criminal liabilities. The Court identified four parties as participants in the Internet realm, including the ISPs, website owners, content providers and users or final addressees of the service. Regarding ISPs, the court concluded that as they allow Internet users to connect to the web, without their existence no felony or illegal act could be committed Therefore, the court ruled that a ISP should adopt all necessary technical measures to prevent content providers displaying any illegal or immoral content. The court ruling does not constitute a mandatory precedent for other cases, and other courts may decide a dispute over content displayed on the Internet in a different manner[12].

> **"The computer crime bill of the Senate in Argentina provides that ISPs will be required to collect and store traffic information for a period of two years."**

Another judicial decision that is being appealed this year in Brazil ruled that the Internet auction site arremate.com.br was liable in a contributory way for trademark infringement by allowing onto its auction site the images of counterfeited products of Montblanc and Cartier that had been posted by third party users. The auction site was obliged to pay damages under section 159 of the Civil Code. The decision has been criticised because it would impose an obligation of monitoring content and pages to all Internet service providers. This task is very difficult when the ISP has millions of users.

Requirements for monitoring of pages, communications and actions of users including data retention.

The computer crime bill of the Senate in Argentina provides that ISPs will be required to collect and store traffic information for a period of two years. They may be required to provide this data to judges in the framework of a criminal investigation, by reason of "the protection of public security or national defense" upon requirement of a judge or a prosecutor. ISPs are required to store information enough to locate a terminal computer in a network, the moment the communication was initiated and its origin. In no case the information may be used for purposes other than those expressed in the law. Violation of this law by an ISP is subject to a fine from $ 5.000 to $ 50.000 (U$S 16.600 aprox.) (see section 7 of the senate computer crime bill).

In Chile, there are no laws that would force ISPs to work as censors of the contents accessed by their customers. In a very interesting ruling issued in December 1999, the court of appeal of Concepción, in a constitutional protection case, has found that the responsibility derived from a publication in the web belongs to the "content provider" (or author) when said contents are illicit or harmful. The service provider would only be responsible in the event that, knowing of the illicit activity of a customer, it has not deleted the data, or not prevented access, because it is the only entity that can provide the identity of the persons responsible[13].

Obligation to use or provide filters.

In Argentina, a law in the city of Buenos Aires (law 863) was enacted in September 2002, mandating the use of filters in local stores and shops that provide access to the Internet (e.g. cybercafes). The law provides that they must install filters in their computers to avoid minors accessing pornography. Filters must be deactivated if an adult is using the computer. Fines for violating this law are up to 1000 pesos (aprox. U$S 300). The Mayor of the City of Buenos Aires has not yet issued regulations implementing this law. A similar law was enacted by the legislature of the City of Jujuy, in a province located in the North of Argentina. Another law at the national level (Law 25.690) was approved compelling ISPs to provide filters to its subscribers upon request.

In Peru a national Law[14] restricting access to minors was enacted in June 2003. The new law provides that companies of public cabins for access to Internet or cybercafes must install in their computers specific software to restrict access to certain web sites containing information considered "pornographic, erotic, contrary to

moral or good customs or against the moral and psychological integrity of children or affecting the family or individual privacy" (section 1). Each establishment must have at lest two computers with specific software that must be assigned to minors (section 2). Municipalities and Prosecutors are in charge of the compliance of the law (section 3). Municipalities must also initiate a campaign of registration and the implementation of a database. Only those registered in the database are allowed to have access to Internet. They must exhibit in their shop or local a logo of compliance (section 4). The bills that formed the basis of this law were strongly criticised by the different associations of ISPs in Peru[15].

> **"ISPs are required to denounce to the authorities any criminal act against minors that comes to their attention, including the existence of pornographic material"**

After the enactment of this legislation many municipalities have enacted similar laws. The Municipal Ordinance no. 155 of the County of Jesus Maria (Peru) was enacted in July 2003[16]. The owners of "cabinas publicas de Internet" (public Internet cabins) must provide places only for minors in their shops with "mechanisms to filter pornography and violence". The owners of public cabins must also install in their computer a screen saver with the logo of the municipality mentioning the ordinance. Similar ordinances started to be enacted in other municipalities[17].

In the year 2001, Colombia enacted law 679 for the prevention of pornography[18]. In chapter two, the law refers to Internet usage and establishes the creation of a commission of experts that shall have the obligation to elaborate a catalogue of abuses of minors by way of the Internet. The Commission will propose technical measures such as filters, classification of sites and blockage of contents that may harm minors in Internet. The report is due to be completed by the end of 2003 (section 4).

It also provides that with that report the national government shall adopt all necessary administrative and technical measures to prevent the access by minors to any pornographic information and to avoid the use of the Internet to sexually exploit children (section 5).

Section 6 provides that the government, through the Ministry of Communications shall promote the use and adoption of self-regulatory systems and codes of conduct in the use of Internet. These codes must be elaborated with the participation of ISP's and users (section 6).

Section 7 forbids ISP, users and administrators (i) to host in their web sites images, text, documents or audiovisual files related directly or indirectly with sexual activities with minors; (ii) to host in their web sites pornographic material, specifically images and videos, when there are indications that the persons photographed of filmed are minors and (iii) host in their own web site links to other sites that contain or distribute pornographic material related to minors. Minors are persons under 18 (section 2).

ISPs are required to denounce to the authorities any criminal act against minors that comes to their attention, including the existence of pornographic material; and establish technical means so users can block for themselves and their children any illegal material (section 8). The Ministry of Communications will receive the complaints of violation of this law (section 9) and impose sanctions on ISPs. This obligation may imply some level of surveillance over web sites.

Finally, a bill was introduced in the Argentinean Congress in the year 2001 establishing requirements that users' activities be logged in cybercafes and "locutorios".-

Intellectual property/Copyright issues

In Colombia, the Penal Code (section 272) provides a DMCA-style provision but it has not been applied so far to any Internet web site.

> **"Due in part to weak online security or lack of employee confidentiality it is very easy to obtain personal information from companies or the government"**

Although peer-to-peer networks are not illegal per se, the copying or non authorised reproduction of copyrighted works is a civil and criminal act in most of the Latin American counties[19].

There have been many cases of removal of domains due to trademark laws and names laws in Latin America (both at the level of national courts as well as at the level of international arbitration at

WIPO). But all these case are related to IP conflicts and none of them have a direct connection to freedom of speech (e.g. there have not been any cases related to "suck domain names", or criticism of companies or government using parody sites, etc).

Finally, ISPs can be required to give over user information due to copyright infringement and this has happened in cases related to commercial email (see next section).

Privacy issues

There are some countries with data protection law such as Argentina, Chile, Peru or Paraguay and others - Brazil, Mexico, Peru and Uruguay - have moved to introduce data protection bills.

ISPs do not use their customers' information for other commercial purposes. In countries like Argentina, Chile or Mexico the law restricts them using this information for other purposes. But if the information is requested by a judge they will have to provide it. For example, a company in Argentina was able to obtain an order of a civil judge requesting the ISP to provide the identity information of a user who had spread via email a rumor against the plaintiff company. The judge granted the order and the plaintiff obtained the identity of the person using a "diligencia preliminar" (a legal procedure aimed at obtaining evidence before starting a trial).[20]. After learning of the future lawsuit through this procedural measure, the individual stopped sending the email that accused the company of environmental pollution.

Although ISPs try to preserve confidentiality of their records, it is common to see in the Internet new pirate databases of email or electoral roll data being offered. Due in part to weak online security or lack of employee confidentiality it is very easy to obtain personal information from companies or the government, as demonstrated by the ChoicePoint case (involving public records from Argentina, Brazil, Colombia, Mexico, Costa Rica and Nicaragua).

Cryptography and cryptography products are widely available from the Internet and there are no restrictions in Latin America on their use. It is common to see people using PGP or other security programs with encryption capabilities.

Legal requirements for ISPs to build surveillance and wiretapping capabilities are becoming more common. The intelligence law of Argentina stipulates in a detailed fashion how private telecom companies must collaborate with the intelligence agencies to wiretap communications. The computer crime bill will establish data collection obligation for ISPs.

Digital divide issues

Most Latin American governments have privatised their public telephone companies and established universal access obligations in the privatised legal regimes. Although Internet connectivity is not directly contemplated, the general obligations relate to the implementation of minimum telephone lines per inhabitant, which is, of course, a prerequisite for access to Internet.

"Legal requirements for ISPs to build surveillance and wiretapping capabilities are becoming more common"

In some cases, this obligation is found in the Constitution. For example, the Constitution of Venezuela provides that the Government must provide and guarantee public services of radio and television and library and computer networks with the objective of assuring universal access to information[21].

Percentage of the population with access to the Internet

In the year 2001 it was calculated that in Latin America there were 25.33 million individuals with Internet access (NUA Survey 2001). The leading countries are Brazil, Mexico and Argentina (CyberAtlas). According to Pesquisa Internet Brazil (5th edition) only 3,3 million of the surveyed population of 36 millions persons use computers to access the Internet. Many countries are developing plans to increase Internet presence and access to electronic resources. Brazil has increased it presence on the Net due to a national plan. Peru has also established kiosks in public places. Broadband connections to the Internet are only available in big cities and most of the connections are dial up.

Position of the government on access to government records online

Some governments in Latin America have started to post information online to give their citizens more access to public data and to promote transparency.

For example, Peru has a portal maintaining all public information about government (see perugobierno.gob.pe) and another portal related to economic transparency showing how the government spends money (transparencia-economica.mef.gob.pe). In Argentina a similar portal (www.cristal.gov.ar) was launched in the

year 2000 aimed at bringing transparency to the public administration[22], implemented by Law 24.156. Peru, Mexico and Paraguay have freedom of information laws.

Footnotes

[1] See Base de Datos Políticos de las Américas (1998) Libertad de pensamiento y de expresion. Análisis comparativo de constituciones de los regímenes presidenciales. [Internet]. Georgetown University y Organización de Estados Americanos, at: http://www.georgetown.edu/pdba/Comp/Derechos/pensamiento.html. 11 (visited 11/8/003) and also http://www.constitution.org/cons/natlcons.htm.-

[2] The American convention has been ratified by the following contries: Argentina, Barbados, Bolivia, Brazil, Chile, Colombia, Costa Rica, the Dominican Republic, Ecuador, El Salvador, Grenada, Guatemala, Haiti, Honduras, Jamaica, Mexico, Nicaragua, Panama, Paraguay, Peru, Suriname, Trinidad and Tobago, Uruguay and Venezuela.-

[3] See www.cidh.org/Relatoria/English/FuncObject.htm

[4] Although there may be excepctions. See Office of the Special Rapporteur for Freedom of Expression, Report on the situation of the freedom of thought and expression in Haiti, at www.cidh.org, and also coutry reports for Panama (2003), Paraguay (2001) and Peru (2000).

[5] See The legal initiative for Internet censorship in Chile, Silencing the Net – Recommendations, http://www.oneworld.org/news/partner_news/hrw/hrw9.htm

[6] See Latin American Internet Legal Compendium, latin American Alliance, LLP, pag. 10.

[7] See decision and comment to the case at www.ulpiano.com/boletin9.htm.

[8] see Annual report of the Special Rapporteur for Freedom of Expression 2002, at ¶ 68 (avalable at www.cidh.org).

[9] See Bianchi and Gullco, El derecho a la libre expresion, LEP, Buenos Aires, 1997, p. 92.

[10] See Margarita Valdes Cortes, Internet Censorship around the world (325), University of Chile, Proceedings of the conference Inet 2000. This information is taken from http://www.isoc.org/inet2000/cdproceedings/8k/8k_4.htm

[11] http://www.bmck.com/elaw/archivehome.asp, (visited August 11, 2003).-

[12] See E-commerce in 21 jurisdictions worldwide, 2001, section Chile, by Carey & Cia. Ldta published by Law Business Research Ltd, p. 26.-

[13] See Margarita Valdes Cortes, Internet Censorship around the world (325), University of Chile, Proceedings of the conference Inet 2000, at http://www.isoc.org/inet2000/cdproceedings/8k/8k_4.htm

[14] See Ley que restringe el acceso de menores de edad a paginas web pornograficas en cabinas de interent a traves de software especiales, available at www.aspesi.net/leyes.htm (Aspesi is the Asociacion Peruana de Empresas de Servicios de Internet).

[15] See letter to Congres in www.aspesi.net/Nota%20de%20Prensa.htm

[16] See "Menores ya no accederan a paginas pornograficas" http://cabinasperu.com/community (Visited 16/08/2003).

[17] See http://cabinasperu.com/community

[18] See text of the statute at www.hfernandezdelpech.com.ar

[19] See IP Legislation Database at www.wipo.int

[20] See Juzgado Nacional de Primera Instancia en lo Civil N° 91, "Shell Compania Argentina de Petroleo S.A. s/ diligencia preliminar", providencia del 4/3/99.

[21] See Artículo 108. Los medios de comunicación social, públicos y privados, deben contribuir a la formación ciudadana. El Estado garantizará servicios públicos de radio, televisión y redes de bibliotecas y de informática, con el fin de permitir el acceso universal a la información. Los centros educativos deben incorporar el conocimiento y aplicación de las nuevas tecnologías, de sus innovaciones, según los requisitos que establezca la ley. See http://www.georgetown.edu/pdba/Constitutions/Venezuela/ven1999.html

[22] See http://www.cristal.gov.ar/Englishindex.html

Argentina

Article 14 of the Argentine Constitution assures "all the inhabitants of the Nation" the right "to publish their ideas through the press without previous censorship". Furthermore, Article 32, which is based on the First Amendment of the U.S. Constitution, provides that "the Federal Congress shall not enact laws that restrict the freedom of the press or that establish federal jurisdiction over it". After the constitutional reform of 1994, Section 22 of Article 75 of the Argentine Constitution conferred constitutional hierarchy to several international documents, including the American Convention on Human Rights (ACHR).

Internet usage in Argentina is growing and it is becoming a new medium of expression. Individuals are starting to use the net to promote ideas and publish news, to criticise government policies; governments are using it to publish bills and legislative proposals open for public comment.

In 1997 the government approved a sort of anti-censorship decree (Decree 1297/97) after the Communications Decency Act (CDA) was struck down by the Supreme Court of the United States. The decree of the Executive Power quoted in its recitals the "ACLU v. Reno" decision of the U.S. Supreme Court, and it provided that freedom of expression applies to the net, as it should with any other medium.

At the end of 2002, Law 25.690 was approved compelling ISPs to provide filters to its subscribers upon request. The law was a surprise to the ISP community in Argentina1. They complained of the lack of consultation, the lack of funding to buy software filters and a possible overly broad interpretation of the law. Furthermore, the law does not define what is forbidden: it merely provides that ISPs are required to provide to its users programmes that "impede access to specific web sites", leaving to a regulation – yet to be enacted - what web content will be defined. Initially the bill was drafted to require ISPs to provide filters only for adult content2, but the change in the law has led critics to argue that government may be able to forbid anything under this broad statement of the law (e.g. certain religions government dislikes or discriminatory acts, etc).

Further legislative developments relating to Internet censorship have occurred at the regional level. The city of Buenos Aires enacted a law (law 863) in September 2002, mandating the use of filters in local stores and shops (e.g. cybercafes). The law provides that they must install filters in their computers to avoid 18 old minors accessing pornography. Fines for violating this law are up to 1000 pesos (aprox. U$S 300). The Mayor of the City of Buenos Aires has not yet issued regulations implementing these laws. A similar law was enacted by the legislature of the City of Jujuy, a province located in the North of Argentina.

The only hate speech prosecutions related to the net were initiated by an Argentine who had pending litigation with the local Yahoo site (Yahoo.com.ar) over the right to use that name. Contemporary to the French "UEJF v. Yahoo" ruling, he denounced that Yahoo was violating the anti-discrimination law no. 23.592. The judge dismissed the claim and the Federal Court of Appeals (of San Martin) affirmed the dismissal with an extensive report from the prosecutor explaining why the Yahoo auction site was not violating the anti-discrimination law. "The ban to an offering of nazi memorabilia in the internet site will be the equivalent of banning the sale of a book of the nazi era in a bookstore" said the Prosecutor.

Another case in the year 2002 dealt with the right to disseminate ideas contrary to the criminal policy of the State. Two individuals, Matías González Eggers (owner of www.fasito.cjb.net) and Leonardo Vita (www.cannabis.com.ar) developed two web sites dedicated to criticism of the law that criminalises possession of marihuana. A federal judge indicted the owners of the sites under a statute that sanctions the "public promotion of the use of drugs" but the Federal Court of Appeals reversed the decision. The court asserted that the fact that setting up a web site with links to other sites were different uses of marihuana are shown is not a violation of the law. "We cannot punish the publication of ideas in the internet that criticises the criminal policy of the government because that is against freedom of expression". The court based its decision in articles 14 and 32 of the Federal Constitution and the ACHR. The Prosecutor appealed the dismissal decision and in the year 2003 the Court of "Casación" revoked this decision. The Court concluded that all the elements of the crime were present and that there was a need to apply the criminal code to the case (see decision of March 24, 2003, by the Fourth Chamber of the "Court of Casación").-

Finally, a decision of the same Federal Court of Appeals protected the sources of the Financial Time's Buenos Aires correspondent, Thomas Catan, who sparked a political storm leading to a judicial investigation when he reported allegations of bribery in Argentina's congress in August 2002. Catan cited unnamed sources, who claimed some Argentine senators had sought cash payments from foreign bankers in return for voting against legislation that would levy a

new tax on banks. A federal judge subsequently ordered the seizure of Catan's telephone records but a federal court ruled later that, in doing so, the judge violated press freedom. The court of appeals ordered the destruction of telephone records seized from the journalist. "The records could potentially reveal the journalist's sources, and the court gave a public reprimand from a higher appeals court for his disregard of Article 43 of the Argentine Constitution, which guarantees the journalist's right to protect sources" said the court.

In 1999, the Criminal Appeals Court in Buenos Aires found that the privacy in the Criminal Code includes the protection of stored files and electronic mail from being viewed without the users permission. The Ministry of Justice is currently drafting a law on cybercrime following a Supreme Court recommendation to enact a new law after a federal judge ruled that the 1921 criminal code did not include cybercrimes.

References

Law 25.690 – ISPs must provide filter to its subscribers.
http://infoleg.mecon.gov.ar/txtnorma/81031.htm

Decree 1297/97. Freedom of expression in Internet is protected in Argentina.
http://infoleg.mecon.gov.ar/normas/47583.htm

Law 863 of the city of Buenos Aires.
http://www.cedom.gov.ar/es/legislacion/normativavigente/leyes/html/ley863.html

Law 23.592
http://infoleg.mecon.gov.ar/txtnorma/texactley23592.htm

ADEPA- Asociación de entidades periodísticas Argentina.
http://www.adepa.org.ar/inicio/inicio.asp

Comunicado de ADEPA sobre el caso Thomas Catan
http://www.adepa.org.ar/libertaddeprensa/dcl2.asp

Court rules judge violated press freedom in FT case
http://media.guardian.co.uk/medialaw/story/0,11614,822522,00.html
http://www.todocannabis.com/archivo_notas/noticias_2.htm

Fronteras Electrónicas de Argentina
http://www.ulpiano.com/EFA.htm

Footnotes

[1] See critics at "Denunciamos censura del gobierno" at www.seprin.com/menu/notas2041.htm

[2] See original text of the bill at www.seprin.com/menu/notas2041.htm

Brazil

According to a June 2003 study carried out by IBOPE (Brazilian institute of Statistics and Public Opinion) 7.992 million Brazilians use the Internet in their homes and about 8 percent of the population are considered Internet users. The government has created an Executive Committee for Electronic Government in order to improve access. The Ministry of Planning, Budget and Management has the attributions of an executive department and provides the necessary technical and administrative support for the Committee to work. Its purpose is to formulate policies, establish guidelines, coordinate and articulate implementations to Electronic Government, with the aim of providing services and information to citizens.

The 1988 Brazilian Constitution guarantees "freedom of intellectual, artistic, scientific and communication activity" and expressly forbids censorship of "political, ideological or artistic nature". The Constitution also states that access to information is guaranteed to everyone, except when professional practice requires the protection of information. It also establishes that confidentiality of mail, telegraph and telephone communications is inviolable, unless a Judge issues a warrant for the official accessing of information in order to clarify facts relating to a crime, under the conditions and using the methods established by law.

A number of bills relating to the information society have been proposed but none have been adopted. Where legislation has not been updated to deal with computer crime, traditional legislation is often used to prosecute crimes committed with the aid of ICTs in Brazil.

One legislative initiative that has been developed in response to the advance of the Information Society is the bill that regulates spam in Brazil. This bill sets limits to the sending of unsolicited messages and provides criteria that help users identify the origin of the messages and to block them. The bill of n 6.210, of authorship of Deputy Ivan Paixão proposed on March 05, 2002 for approval in the Congress was not voted upon. There is also a bill proposed by Congresswoman Iara Bernadi that intends to forbid anonymity on web pages and in electronic addresses. Another bill proposes regulations concerning the protection and treatment of personal data, in order to retain individual guarantees of privacy and to establish regulations governing the organisation of databases.

There are no regulations regarding the protection of information. Some observers believe this is because the Executive has neither efficient services nor appropriately qualified civil servants. Many systems are handled by third parties with minimum control from the state. The number of databases containing personal data is increasing in Brazil. These databases tend to be incomplete, inefficient, are not updated and often violate the privacy of users, making them vulnerable to attacks by those with harmful intentions. The Deputy Orlando Fantazzini (Labor Party) introduced a bill in 2002 establishing norms for the protection and treatment of the personal data and other providences, however it still was not voted. Database of financial entities, social organisations, political parties, unions, and government are sold through the Internet with ease, or given, without the data subject's consent, to other agencies or companies that use it for sale of their products. This occurs without any State control.

Antônio de Pádua Ribeiro, President of the Supreme Court of Justice decided that an Internet user was not allowed to send an e-mail because it libeled the image of her ex-husband. The Internet user declared that the ruling of the Court of Justice violated her right to e-mail confidentiality since the message was read by the court in order to verify its contents.

Recently, it was discovered that the author of the web page, which libelled former governor Cristovam Buarque and the Labor Party, was Stannley Jacinto Vasconcelos who belongs to an opposition party. The investigation has not been closed. The police are waiting for an order to break the confidentiality of two accounts of free providers in the United States in order to know if there is someone else involved in the crime. The document with the information asked by the Delegacia de Crimes pela Internet de São Paulo (Internet Crimes Police Bureau of San Pablo), which has national jurisdiction and investigates the web site by request of Cristovam's advisors, should shortly be received by the commissioner Mauro Marcelo de Lime e Silva. By request of two representatives of the PT, the Chamber has created two committees in order to conduct a parallel investigation.

One of them, which comprises three computer technicians, will take a deeper look at the computers of the House. The other, composed of some of the Chamber employees, will listen to the statements of workmates of the computer section and all Pirineus' advisors. This commission has 15 days to complete these tasks. Cristovam, the PT and Maria José Maninha –who is also mentioned in the website – will present an action against Stanlley, Pirineus and the PMDB. They want the responsible people to be charged with three

crimes: calumny, libel and injury. All three crimes have penalties of between six months and two years imprisonment.

References

http://www.ibope.com.br/

http://conjur.uol.com.br/textos/20248/

http://www.estado.estadao.com.br/editorias/2000/12/06/pol137.html

http://www.planalto.gov.br

Costa Rica

According to an October 2002 study carried out by CID Gallup, 110,000 homes in Costa Rica are connected to the Internet. There are more than 220,000 users, 70,000 of whom use the Internet every day. 10 percent of the population are considered Internet users and, according to the national telecommunications operator, it is hoped that these figures will jump to 20 percent by the end of 2003.

The Costa Rica Constitution protects freedom of speech and the right to access information in the public interest (except for 'State secrets'). Privacy of data and communications are protected by a 1996 amendment to the Constitution that guarantees the right to intimacy, freedom and secrecy of communications.

On November 12, 1999, the Penal Court of the First Judicial Circuit in San José convicted the journalist, Herrera Ulloa and the daily La Nación of criminal defamation based on 1995 articles by Ulloa that cited European press reports alleging corruption by former Costa Rican diplomat Félix Przedborski. The Third Chamber of the Supreme Court upheld Ulloa's sentence of 120 days in prison and a fine, and ordered his name to be inscribed in the Judicial Criminal Register. In addition, because it published the story, the newspaper La Nación was ordered to pay the legal fees of the plaintiff's attorney and to "remove the link to the digital version of the newspaper on the Internet, between the surname Przedborski and the impugned articles, and to establish a link between these articles and the resolution of this verdict".

After the Costa Rican Supreme Court rejected La Nación's appeal, the journalist filed a petition with the Inter-American Commission on Human Rights, an entity of the Organization of American States (OAS), which ordered the Penal Court to delay its ruling until the commission had studied the case. The court refused and the commission filed a complaint with the Inter-American Court, which issued a stay In an unprecedented decision, and the first case against Costa Rica, the Inter-American Court of Human Rights issued an order on September 7, 2001 that Costa Rican authorities desist from enforcing certain sections of the 1999 defamation verdict. Decisions of the court are legally binding on Costa Rica and other countries that have accepted the court's jurisdiction.

The Commission maintains that the alleged acts could constitute "irreparable damage" to the human rights of the journalist, Herrera Ulloa and Mr. Fernán Vargas Rohrmoser of the daily La Nación, as well as irreparable damage to the Costa Rican citizens who have been deprived of access to information regarding the actions of public officials. At the time of writing, the commission was still studying the case.

The Patent of Inventions, Industrial Models and Designs and Utility Models Act states that "discoveries, scientific theories, mathematical methods and computer programs considered in isolation are not considered inventions.". The Copyright and Related Rights Act, however, gives protection to "computer programs including previous versions and derived programs".

There is a Bill concerning personal data protection inspired by the European law. In several cases the Supreme Court's rulings filled the legal gaps surrounding personal data protection.

In October, 2001, some reforms were introduced into the Penal Code in order to include wiretapping (article 196bis), computer fraud (article 217bis), and alteration of information and computer sabotage (article 229bis).

Also there is a bill of law on freedom of speech and press. It is a proposed law which tries to make the freedom of speech and press more extended. Some improvements to the criminal law and to the civil code are set forth, so as to update the legislation on these matters.

References

Boletin No. 100. Sala Constitutional Junio 2002. Acceso a Informacion Electronica. http://www.poder-judicial.go.cr/salaconstitucional/boletines/100.html

October 2001 law amending Penal Code http://www.racsa.co.cr/asamblea/ley/leyes/8000/8148.doc

Peru

Approximately ten percent of the Peruvian population has access to the Internet. The vast majority of these people live in the western La Costa region which makes up about 10 percent of the country. Communications are difficult in the other two regions.

The most common way to access to the Internet is through Internet booths. There is a low level of computer penetration in private homes. The Peruvian government has established the FITEL Program (Telecommunications Investment Fund), which is responsible for promoting universal access. The FITEL fund was created to fund the provision of telecommunications services to rural areas and places considered of social interest such as poor urban areas.

Act 27806, the Transparency and Access to the Public Information Act includes the creation of public information portals and considers governmental information as accessible to citizens.

Article 2 of the Peruvian Constitution establishes the right to freedom of expression and freedom from any hindrance of that right, including freedom from censorship. There are not generally restrictions on Internet Content in Peru. There were temporary restrictions in 1998 in accessing the web pages of Sendero Luminoso and the MRTA (both terrorist movements opposed to the government). Hosted on servers outside Peru, these websites were inaccessible through some ISPs, but the filtering was more a matter of social pressure than official regulations. Although there are no regulations to control Internet content, there is an act that forbids statements defending crimes (especially terrorism) which could be used to restrict access to certain websites. Bylaws that forbid the access of minors to pornography at Internet booths have recently been established.

The Intellectual Property Act applies to the Internet. There are some cases related to the use of content by third parties, although these cases involved copyright protections more than censorship mechanisms. ISPs in Peru are responsible for the content hosted for their clients, and thus may avoid the publication of content for fear of liability. A case in which the owners of an ISP were accused of hosting a website that they were aware was violating the intellectual property of another was settled out of court. Some domains, such as Aerocontinent.com and cablemagico.com, were removed due to their infringement of copyright laws.

In 1999, a group of journalists were libeled in a web page (http://www.aprodev.org), which was operated by unknown persons. This page was an instrument of the dictatorial government of the then President Fujimori to discredit his opponents. The case did reach the courts but the judges refused to hear the case because the organisers could not be identified.

Regarding specialised regulation on the access to other people's information concerning crimes, the Communications Control Act (Act N 27697) allows the public prosecutor, in exceptional cases to interfere with and to control communications and private papers.

References

FITEL
http://www.fitel.gob.pe/

ORDENANZA MUNICIPAL Nº 000007 Establecen restricciones para el acceso a páginas de contenido pornográfico a través de cabinas públicas de Internet
http://www.aspesi.net/ord-sanjuan.htm

Ley No. 6 de 22 de enero de 2002 Que dicta normas para la transparencia en le gestión pública, establece la acción de Hábeas Data y dicta otras disposiciones.
http://www.asamblea.gob.pa/legispan/leyes/2002/2002_006.pdf.

Ley 27697. Communications Control Act
http://www.alfa-redi.org/documento/data/63.asp

Las Extrañas Influencias de Faisal
http://www.caretas.com.pe/1999/1568/controversias/controversias.htm

Bills relatinng to the Sociedad de la Información
http://www.alfa-redi.org/asic/epsilon.asp

Uruguay

Approximately 12 percent of the Uruguayan population has access to the Internet. About 49% of those connect to the Internet at their place of work; 55% are male, and the vast majority are under 30. There are very few privately managed telecentres but the national telecommunications company, Antel has plans to franchise 100 telecentres and 100 telephone booths mainly located in the capital, Montevideo and on its outskirts.

The Uruguay Constitution of 1967 protections the rights of privacy and free speech.

Several groups affirm that self-censorship is the most common problem on the Internet in Uruguay. Several minority groups use the Internet within the legal framework and without censorship by the authorities. Very few cases of overt censorship have been identified, and those that have are mainly due to pressure on journalists from media owners.[1]

The 1989 Communication and Information Act defines mass media crimes as "(a) the disclosure of false news, knowing it is untrue, which causes a serious disturbance to the community or serious damage to the economic interests of the State or to its foreign credit; (b) the instigation of an offense to the Nation, the State or its Powers." Punishable persons include, those who publish or distribute information containing false accusations, or information that challenges the state, or information concerning adultery and divorce, or processes related to crimes of indecent assault or indecency.

Senator Pablo Millor presented a bill in 2002 to modify the Criminal Code with a new definition of "home disturbance" to include revelations about corrupt politicians and businessman ("escrache") who were involved in previous military governments. The dissidents' practice includes the spreading of escrache images and contents via the Internet. Protests are then organised in front of the houses of public figures. The bill is still pending.

The Patents Rights and Duties Act of 1999 establishes that computer programs (considered in isolation) and different ways of reproducing information are not considered inventions. There is a bill concerning software copyrights that proposes that "Software are protected .... in the same way as literary works are".

The Criminal Process Code of 1980 regulates wiretapping and the interference of personal communications as such: "If there are strong reasons to believe that the interference with the correspondence or any other means of communication in which the defendant takes part, even if he does it using a fictitious name, would provide useful information for verifying the crime, the Judge may order it and will arrange its seizure" (article 212).

References

Anti-escarches Act
http://www.parlamento.gub.uy/HtmlStat/PL/Fichas/Asuntos/Ap20753.htm

Ley N° 15.032 Criminal Procedure Code on wiretapping
http://www.parlamento.gub.uy/leyes/ley15032.htm

Internet Censorship in the Middle East
Regional report

The Middle East region exhibits a complex approach to the Internet and to freedom of expression in general. Governments of some of the largest nations, such as Saudi Arabia, tend to regard the medium with suspicion, and have been slow to build an Internet infrastructure. The governments of others, such as Bahrain and Jordan have taken a more economically pragmatic view, adopting the technology in a range of sectors. Nonetheless, all governments in the region have had to carefully consider the effects of having an increasingly informed general public. They have also been influenced by what some perceive as a conflict between national or traditional culture and values and anything that could be interpreted as a threat to such values.

> **"The Internet in the Middle East, as in many other regions, has offered support to those who wish to express their opinion freely and engage in democratic debate."**

The Internet in the Middle East, as in many other regions, has offered support to those who wish to express their opinion freely and engage in democratic debate. To many it can be seen as a movement towards the development of a democratic region. The medium has provided opportunities for citizens to participate in democratic forums, and to discuss and debate the political, social and economic issues that concern them. Unlike other media where the information flow is unidirectional – from the government to the masses - the Internet allows a multidirectional communication process that offers the opportunity for those who have access to the medium to interactively engage with others. The development of the Internet has thus lead to more horizontal and less vertical means of communication.

Because of relatively low penetration levels, some observers are doubtful as to whether the Internet can affect the development of democracy in the Middle East in any significant way. What is clear, however, is that, for the first time in history, the people of the Middle East now have the means to stimulate the development of democracy. This is, however, no more true for the people in the Middle East than for most of the world.

Development of the media ecology in the Middle East has for the past 40 years been shaped by the policies of authoritarian regimes as well as by commercial imperatives. The media in the region is, in general, controlled and monitored closely by governments - either by direct ownership or through strict laws and regulations that direct the media agenda. The major role of the media in the Middle East is as a propaganda tool to promote the government's political, cultural, and economic programs. Since the eighteenth century, the media has operated in an environment of direct censorship by the state and self-censorship by journalists, editors and publishers. Many journalists in the region are convinced that the authorities are using new monitoring and surveillance technologies to record their actions and ultimately punish them if they transgress established policies. The media thus continues to favor protocol news in which content registers state power and enforces national political solidarity. The Middle Eastern media remains largely composed of government monopolies, with the advent of the Internet and new communications technology being viewed by governments in the region as yet another platform to publicise their viewpoints.

> **"Because of relatively low penetration levels, some observers are doubtful as to whether the Internet can affect the development of democracy in the Middle East in any significant way."**

Internet Development in the Middle East World Internet technologies first arrived in the Middle East in 1992 when Egypt established its first connection through France. Several Arab states then started joining the newly-networked world with the result that communication technology in some communities, such as Saudi women's use of the Internet and the uptake of the mobile phone in Egypt, have been embraced and welcomed – even if it is only the wealthier communities that have access. As of May 2003, every country in the region - except Iraq and Libya - had some form of Internet connectivity. Members in all of these countries could connect to the Internet in some fashion via local Internet Service Providers (ISPs). According to 2003 statistics, there are nearly 9 million Internet users in the Middle East with an Internet penetration of 2.2 percent - less than

half of the world average of 5.2 percent. The United Arab Emirates has the highest penetration in the Middle East with 20.4 percent of the population having access to the Internet. Saudi Arabia and Egypt are a distant second and third with penetration rates of 2.6 and 2.2 percent respectively.

> **"Many journalists in the region are convinced that the authorities are using new monitoring and surveillance technologies to record their actions and ultimately punish them if they transgress established policies."**

While the Gulf States of Qatar, Kuwait and Oman possess the financial strength and state-of-the-art technological capacity to promote their Internet infrastructure, the number of Internet users is growing more slowly here than in other countries with far weaker economic capacities such as in Egypt and Jordan. Middle Eastern Internet analysts have determined that low Internet penetration in the Middle East exists due to a number of factors relating to weak infrastructure, poor economic growth, high illiteracy levels, lack of relevant language, content and applications as well as cultural factors.

Firstly, a relatively weak telecommunications infrastructure hinders the wider adoption of the Internet. Though some Middle Eastern telecommunication indicators can be compared with those of developed countries, overall poor networking capacity in the region has led to low usage and high Internet costs. In most cases, this infrastructural dilemma is the responsibility of state-run telecommunication companies, with the capacity and quality of the different networks varying from country to country. In 1995, there was an average of four telephone connections per 100 inhabitants, which is one-tenth the amount of most industrialised countries. However, several Middle Eastern countries, for example Syria, have thoroughly modernised their telephone networks and have ordered extensive expansions during the past decade. Countries such as Egypt or Oman are consequently registering some of the highest increases in telephone connections worldwide.

Poor economic growth is another problem facing Internet development in the Middle East. Low income is a key factor hindering the widespread use of the Internet in the Middle East. The cost of Internet access and usage charges, as well as the associated costs of hardware and software is often prohibitive.

The third problem is seen to be the high illiteracy rate which is currently at a level of between 40 and 60 percent. There also exists a shortage of Arabic and other Middle Eastern language content and applications relevant to the region.

Finally, there are many powerful elements of Middle Eastern government and society that do not readily accept new technologies and allow its diffusion, due largely to its Western origins.

> **"A few Middle Eastern governments have displayed a fairly liberal approach to Internet regulation that has resulted in freer expression online than is permitted in the local news media."**

Internet Censorship

A few Middle Eastern governments have displayed a fairly liberal approach to Internet regulation that has resulted in freer expression online than is permitted in the local news media. Kuwait, Morocco, Algeria, Egypt, Jordan, and Lebanon have all permitted online freedom of speech for Internet users in each country, even as they enforce press laws against print periodicals that publish "objectionable" material. In Egypt and Jordan, for example, newspapers and articles that the authorities censored become quickly available online, thus evading the censorship of traditional media, Morocco, and the Palestinian Authority have made little if any effort so far to control online content, allowing Internet users access to a wealth of information that the local print and broadcast media cannot publish. This is mainly because of the low penetration of Internet technologies in those states where the Internet is seen as creating no threat.

This is not the case for most Middle Eastern states. As previously mentioned, the advent of the Internet has been met by hostility by most governments in the region. Only time will tell whether the people of the Middle East are able to seize the opportunities offered by new technologies in order to promote more widespread use and interaction with digital communication media.

References

Writing for an Arab Internet Portal by Hala Fattah
http://www.georgetown.edu/research/arabtech/fattah.html

Culture Media & the Next Generation in the Middle East, by Jon W. Anderson.
http://nmit.georgetown.edu/papers/jwanderson.htm

http://www.georgetown.edu/research/arabtech/datab.htm

Problems facing Arab media to join the online world
by Ahmed El Gody, paper presented to the Arab US Association for Communication Educators

Is the Internet Islam's 'Third Wave' or the 'End of Civilization'? by Jon W. Anderson in
http://www.press.umich.edu/jep/archive/Anderson.html

Marginal Muslims in Cyberspace The implications of the Web for Traditionalists, and of Traditionalists on the Web for Islam by Mark Sedgwick.
http://www.hf.uib.no/smi/pao/sedgwick.html

Internet in the Arab world: A step towards Information Society by Henner Kirchner
http://www.hf.uib.no/smi/pao/sedgwick.html

http://www.journalism-islam.de/Internet/massmedia.pdf

Bahrain

The Kingdom of Bahrain has grown highly dependent on oil for the development of its economy. The Bahraini government thus welcomed the opportunity for the country to become the Internet hub for the Gulf region by promoting the medium for new business projects. Bahrain is also the proxy hub for neighboring Saudi Arabia, providing Saudi citizens with a path to curb the Saudi government's harsh censorship regime.

Unlike other Gulf countries in the region, the Bahraini government took limited steps to censor the Internet, understanding the importance of Internet freedom for maintaining economic development and investment in the country. Many citizens opposed the Internet's distribution of pornography and gambling declaring that this was eroding Islamic values and morals. The government responded by providing links to free Internet filtering software.

Internet provision in Bahrain is offered by Bahrain Telecom (Batelco), the state monopoly telecommunications company and sole ISP in the kingdom. Batelco started offering public Internet access in 1995. The government requires no authorization for accessing websites, or publishing materials online. The Bahraini law stresses that "no communication shall be censored" nor any "content thereof revealed" except in special cases that can "threaten the system".

However, the government's control over the country's Internet traffic makes it easier for it to monitor and detect "Internet misuse". According to a Human Rights Watch (HRW) report, misuse is defined as "criticizing the rule of the Al Khalifa family". The Bahraini government is aware of Shiite (the opposition party) use of the Internet to disseminate information against them. According to HRW, a number of Bahrainis have reportedly been detained or questioned on suspicion of using electronic means to transmit information to political opposition groups outside the country, some of whom were sentenced to prison.

According to a Reporters Without Borders report, the government has suppressed Internet content critical of its authority by blocking websites and monitoring the opposition's use of the Internet. Opposition parties responded by condemning the government's actions as a blow to freedom of expression. Replying to allegations, the Bahraini government stated that the sites had to be censored after becoming a platform for publishing rumors and lies. The Bahraini Minister of Information, according to the same report, stated that the ban would be lifted if offensive materials were removed from the sites

References

Reporters Without Borders 2003 Internet Censorship Report
http://www.rsf.org/IMG/pdf/doc-2236.pdf

Reporters Without Borders News article: Government blocks websites (27 March 2002)
http://www.rsf.org/article.php3?id_article=942&var_recherche=Bahrain

Human Rights Watch: The Internet in the Mideast and North Africa: Free Expression and Censorship
http://www.hrw.org/advocacy/internet/mena/bahrain.htm

Jordan

The Hashemite Kingdom of Jordan is a constitutional monarchy where the king has widespread powers. He appoints the Prime Minister, members of the cabinet council, as well as a 40-member senate. As a monarchy, the views of the king have a major impact on decision-making which has clearly influenced development of the Internet in Jordan.

Internet services started in Jordan in 1995, at which time connectivity was principally in the hands of the government and academics. Rapidly, these efforts were privatized, and by the following year privileged users understood the role of the Internet in sustaining the economy. Both the late King Hussein and his successor, King Abdullah did much to promote the development of ICTs in the kingdom. This interest fostered the development of a national information system as well as an attempt to link information-generating centres in both the public and private sectors. In 1999, Jordan identified ICT as a goal for the 2020 REACH development vision that was formulated in order to generate foreign investment and thus create a sustainable economy.

Telecommunication infrastructure and regulation has evolved to sustain the development of the Internet in Jordan. Several private ISPs have been granted permission to offer services, although all links must still pass through the government telecommunication hub. Individuals, corporations, and organisations are able to establish Internet accounts easily without government approval or registration. In 2001, the city of Irbid boasted 105 cybercafes on one street alone.

Although Jordan has the highest literacy rate among Arab countries, there are still problems that hamper the diffusion of the Internet in the country. Firstly, Jordan is a relatively poor country where most citizens cannot afford the cost of a PC, modem and Internet subscription. Secondly, all Jordanian ISPs are located in the capital city of Amman, restricting access to urban users and facilitating greater government control over ISPs. Access points outside Amman are only available through slow and expensive long-distance dial-up.

Until September 2001, Jordan was among the few countries in the region that enjoyed relative freedom on the Internet with no regulations and no blocking of sites. Although several conservative elements in society objected to the government's policy of refusing to block pornographic and gambling sites, the Internet enjoyed privileged exemption from the censorship regularly applied to other forms of media.

After September 11th, the Jordanian government enforced censorship and control measures across all types of media, including the Internet. In December 2001, the Higher Media Council was established to reform Jordan's media policies as well as to monitor online behaviour. The body started tracking ISPs and questioning owners about details of banned sites.

In May 2002, the State Security Court sentenced Toujan al-Faisal, the first female member of the Jordanian Parliament to prison for 18 months for "false and exaggerated news that defames the state and undermines its sovereignty". She had accused the Prime Minister on the Arab Times website of doubling the fees on car insurance for personal reasons. She was given amnesty by King Abdullah II but was prevented from running for office in 2003 because of the conviction.

References

Jordan joins debate over Internet access controls, Jordan Times, November 30 - December 1, 2001
http://www.jordanembassyus.org/11302001002.htm

The Landscape of ICT in Jordan
http://www.american.edu/initeb/zt9072a/jordan.htm

Jordan's IT industry to launch the REACH Initiative
http://www.jordanembassyus.org/07112000003.htm

Information Technology Association – Jordan
Reach 2000 Initiative
www.unicttf-arab.org/Doc/Ra'ed%20Bilbessi.ppt

Jordan Times
Tuesday, December 4, 2001
Penal Code to guide Higher Media Council's mandate, says premier
http://www.jordanembassyus.org/12042001004.htm

Higher Media Council trips over as Abu Jaber resigns
http://star.arabia.com/article/0,5596,179_5125,00.html

Jordan: Toujan al-Faisal denied basic rights
http://web.amnesty.org/library/Index/ENGMDE160112003?open&of=ENG-JOR

Jordan sentences Toujan al-Faisal to 18 months for speaking out
http://www.arabicnews.com/ansub/Daily/Day/020517/2002051714.html

The Internet in the Middle East and North Africa. Human Rights Watch
http://www.hrw.org/advocacy/internet/mena/jordan.htm

Qatar

Qatar is the least populous country in the Gulf region, with at least 50 percent the population being foreigners. Most of the Qatari population is located in the capital, Doha.

Qatar was recently in the international spotlight due to the publicity surrounding its influential media organisation, "Al-Jazeera". The Qatari government successfully introduced the TV satellite channel that opened a new platform for freedom of expression in Middle Eastern media by introducing live open forum debates about controversial issues. However, it is believed that this "liberal" approach is only applied outside Qatar's borders since Qatari-based media are still prevented from contradicting the government and its policies.

Internet services were introduced in the country in 1997 through the state monopoly, Q-Tel Telecommunication Company. Shortly thereafter, the Qatari government allowed private companies to provide Internet services to 25,000 users. In its quest to become the media hub of the region, the Qatari government created one of the most sophisticated Internet telecommunication infrastructures in the world. The quality of the Qatari national public switched telephone network (PSTN) is rated as one of the highest by the International Telecommunication Union, and the country has the most modern telecommunications networks in the region, boasting nearly 50 percent excess capacity.

The Qatari government has stated that it will not block any Internet sites and that it will not censor Internet material, declaring itself an "information-open zone". There are claims, however, that Internet censorship is being conducted by keeping an index of prohibited web pages that is regularly updated by Q-tel, by developing special software that blocks "unsuitable" content, as well as by monitoring private ISPs.

References

Media in Qatar
www.tbsjournal.com

National Security and the Internet
in the Persian Gulf Region Executive Summary,
Arab Information Project, Georgetown University
http://www.georgetown.edu/research/arabtech/pgi98-1.html

Response to Human Rights Watch Survey
concerning rules and regulations which govern ISPs.
http://www.hrw.org/advocacy/internet/mena/appendix-c4.htm

Saudi Arabia

The Kingdom of Saudi Arabia is the largest country in the Gulf region. One of the most stable and conservative powers in the Arab world, Saudi Arabia largely dominates decision-making in the region. One of the main goals of the government is to protect the country and its society from "immoral foreign influences". This has a direct impact on the diffusion of Internet technologies in the kingdom.

The Saudi media serves as a hub for peripheral Gulf States. Saudi's private offshore media dominates at least 80% of total Arab media consumption.

For a country as wealthy as Saudi Arabia, it is interesting how reluctant society has been to adopt Internet technologies. Saudi Arabia was the last Gulf state - and among the last countries in the Middle East - to adopt Internet technologies. This occurred in 1994, when only a few medical and academic communities were privileged to have access.

Many critics have declared that this delay was due to the Saudi government's determination to wait for technology to become available that would enable the government to block material that could be of potential harm to Muslim culture and values, including pornographic material, gambling sites and other undesirable "un-Islamic" material.

The first Saudi Internet connection was provided through a US company and censorship over its content was conducted abroad before transmitting back to the kingdom. Saudi citizens and residents were also free to connect to the Internet through neighbouring ISPs, such as Bahrain. In doing so, the Saudi government promoted the goal of implementing Internet technology to assure controlled use of the Internet.

The Saudi government established the King Abdul Aziz City for Science and Technology (KACST) as the governing and regulatory body for the Internet and appointed it with the task of designing the framework within which the Internet would function according to Islamic rules. In 1997, the government commenced feasibility studies seeking avenues to "protect national stability" by careful control of the Internet. In 1999, 71 ISPs were selected to offer Internet service to the community. Most of these companies were government associates loyal to the ruling family.

Soon, more than 100,000 people were using the Internet in Saudi Arabia, with numbers rising exponentially. Within the next three years, more than 1.5 million Saudis had joined the Internet community, the main demand coming from the commercial sector. This increase in the number of users was not, however, matched by the development of telecommunications infrastructure.

The increase in the number of users was met, instead, with more measures to constrain the medium. In a period of three months, KACST blocked over 400,000 websites and established complex technical mechanisms to limit access to foreign Internet hosts and to block not only "immoral websites" but also those belonging to opposition and human rights groups. Many of the filters for this exercise were provided by Western companies such as Secure Computing and Matthew Holt.

In 2001, the Council of Ministers issued a resolution prohibiting users from publishing or accessing data that "infringes the sanctity of Islam and its benevolent Shari'ah", "breaches public decency… contrary to the state or its system" or data that is damaging to the "dignity of heads of states or heads of credited diplomatic missions". ISPs were required to track users' activities in order to enforce the resolution.

In a 2002 study, Harvard University's Berkman Center found that over 2000 sites that they checked for availability were being blocked. They also found "(1) that the Saudi government maintains an active interest in filtering non-sexually explicit Web content for users within the kingdom; (2) that substantial amounts of non-sexually explicit Web content is in fact effectively inaccessible to most Saudi Arabians; and (3) that much of this content consists of sites that are popular elsewhere in the world" (http://cyber.law.harvard.edu/filtering/saudiarabia/).

Business news from the region indicates that Saudi telecoms tycoon, Prince Walid Ibn Tallal is planning

to set up a rival Arab WWW that will only present pre-censored content.

On the other hand, there appears to be an increasing amount of activity in circumventing government restrictions in the kingdom. Some ISPs have hired professional hackers to escape proxy servers in order to connect to banned websites and to surf the web anonymously. Others have started secretly connecting to the Internet via satellite communication networks in order to escape government censorship.

References

Harvard Berkman Center for Internet and Society, Documentation of Internet Filtering in Saudi Arabia
http://cyber.law.harvard.edu/filtering/saudiarabia/

Human Rights Watch Report on Saudi Internet Censorship
http://www.hrw.org/advocacy/internet/mena/saudi.htm

Page to request unblocking of site
http://cgi.isu.net.sa/unblockrequest/

King Abdul Aziz City for Science and Technology (KACST)
http://www.kacst.edu.sa/en/

Council of Ministers Resolution, 12 February 2001
http://www.al-bab.com/media/docs/saudi.htm

Internet Report on Saudi media
http://www.internews.org/arab_media_research/saudiarabia.pdf

Joshua Teitelbaum Middle East Journal, Dueling for Da'wa: State vs. Society on the Saudi Internet, Spring 2002.
http://www.dayan.org/Teitelbaum.pdf

Dr. Ibraheem S. Al-Furaih , Internet Regulations: The Saudi Arabian Experience (govt paper)
http://inet2002.org/CD-ROM/lu65rw2n/papers/u05-a.pdf

BBC country profile
http://cyber.law.harvard.edu/filtering/saudiarabia/

United Arab Emirates

The seven emirates that make up UAE (Abu Dhabi, Dubai, Sharjah, Oman, Umm Al-Qaiwain, Ras Al-Khaimah, and Fujairah) share a single primary supplier of Internet access: Emirates Internet and Multimedia (EIM), a purpose-created division of Etisalat, the national telecommunications carrier. The Sheiks who rule each emirate have extremely wide latitude to govern. Effectively, they can make any laws they want, and there appear to be few complaints, largely because of a widely held assumption, by the general population, that little attention would be paid to complaints.

Etisalat began offering Internet access in 1995 to all categories of users: academic, business, industry and home. By 2001, the number of subscribers had reached 240,000 according to the ITU, but it was estimated that the number of users of those subscriptions numbered 775,000. At the end of 2002, EIM claimed 950,000 users, 39 percent of whom go online from home. Even in 2001, the ITU noted that UAE was the most wired nation in the Arab world, and one of the top nations of the online world overall. Some additional Internet access is available from companies set up in Dubai Internet City or Dubai Media City; these are "free zones", where foreign companies may operate without a local partner. However, the Internet access sold by this route still goes through Etisalat, albeit without the censorship that applies to access provided by EIM. Broadband has begun to roll out in UAE, and EIM claims 19,000 domestic ADSL subscribers as of mid 2003.

Besides private and business subscriptions, Internet access is available via Internet Surfing Centres, which are available in public places such as shopping centres, restaurants, and gaming. As of mid 2002, there were 191 such public access locations, of which 98 were set up in 2002. The majority of users of these centres are, however, the country's large expatriate community.

In late 2002, EIM reported that only about 6 percent of the region's Internet users access the Internet only from work, with 56 percent using it from both home and work. EIM also noted that about 76 percent of Internet users are male, over 60 percent are Asian, and 25 percent are Arabs. Most UAE Internet users tend to be both young and highly educated; users' average age is 27, and 59 percent are college graduates.

Officially, EIM censors only pornography. In its earliest days in 1995, Etisalat operated a single proxy server (proxy1.emirates.net.ae). As the number of subscribers has expanded, EIM has added more such servers. Now, users' Web browsers may be configured to use proxy1 or to turn on auto-configure, which may use any of the proxies. Users note that these servers do not all work exactly the same, so that which sites are censored may depend on which proxy server you are using. In general, the claim that EIM censors only pornography is thought to be fairly accurate. However, some underground sites (for example, some of those offering hacking information) nonetheless do get trapped in the censorship system, usually because they are displaying pornographic ads. Newsgroups are also censored; for example, EIM's Usenet feed (news.emirates.net.ae) does not carry any of the alt.binaries.* newsgroups. Little change has been noted in censorship policy since 9/11.

Dubai enacted an Electronic Transactions and Commerce Law in 2002 which deals with digital signatures and electronic registers. It prohibits ISPs from disclosing information gathered in providing services. The penal code also contains some provisions. It does not address cybercrime or data protection. A cyber-crime act is currently being developed.

Surveillance has not perceptibly increased since 9/11, but has in any case long been at a fairly high level. It is commonly believed in UAE that phone calls are monitored, and most people believe that email and Web use are monitored as well. UAE is planning to begin rolling out biometric ID cards by the end of 2003, and Oman has already begun. There is no forum for opposing this, and because UAE's rulers are not accountable, many other laws are in effect that contravene human rights conventions. For example, non-UAE nationals must renew their residence visas every three to four years, and as part of the renewal process must undergo a blood test. If they are found to be HIV-positive, they are immediately deported.

In August 2001, the UAE also began implementing a biometric system to ensure that unwanted persons do not re-enter the country. It maintains a central database, held by the police, of iris prints; these are taken from anyone who is deported, as well as inmates of prisons and deportation centres. Iris prints from incoming passengers at any of the UAE's six airports or ten sea and land crossings are compared with the database, and entry is refused if there is a match. *Biometric Technology Today* reported in April 2003 that in the first six months of full operation (beginning in October 2002) over 100,000 travellers had been checked and dozens had been caught and denied entry.

References

Personal interview with Mat Beard, editor of several computer magazines in Dubai over the last three to four years.

Al Tamimi & Company , "E-Commerce and the UAE Law
http://www.tamimi.com/publications/ITQuery.htm

ITU 2001 report on UAE Internet access
http://www.itu.int/arabinternet2001/documents/pdf/document25.pdf

Legal Insight to the Dubai Electronic Transactions and Commerce Law No.2 of 2002
http://www.tamimi.com/lawupdate/2002-04/evision.htm

InternetCityLaw.com
http://www.internetcitylaw.com/

Electronic Commerce Laws of Dubai
http://www.tecom.ae/law/

EIM
http://www.emirates.net.ae/

EIM 2002 statistics
http://www.nua.com/surveys/index.cgi?f=VS&art_id=905358485&rel=true

Internet Censorship in North America

Regional overview

Few people would deny that the events of September 11th 2001 have inspired a profound effect on many aspects of international relations, public policy, the military matrix and the world economy. And nowhere, with the exception perhaps of Iraq, has the impact been greater than in the United States. As the reports in this section demonstrate, civil rights that have been taken for granted for so many decades are now under assault both in the US and in Canada.

> **"Civil rights that have been taken for granted for so many decades are now under assault both in the US and in Canada."**

For anyone involved in the arena of communications and IT, that prognosis is almost certainly true. An unsettlingly large number of key political, media and government figures have drawn a connection between communications and privacy technologies and the act of terrorism, resulting in unprecedented pressure on (and by) Congress, the states and foreign governments to regulate and control a range of digital media.[1] The pressure on free expression and other rights in Canada has been profound, a situation made even more fragile because of that country's lesser level of constitutional protections.

This mindset that has driven so many attacks on free expression and open communication was exemplified soon after the attacks by an editorial in the Christian Science Monitor, which observed: "There's some evidence that the perpetrators of the Sept. 11 attacks on New York and Washington had been using e-mail, presumably to stay in touch with each other and further develop their plot. And Osama bin Laden's network has spread its message through CDs and other digital means."[2]

Such bland observations, repeated countless times, have drawn an arbitrary distinction between conventional technologies (the motor vehicle, telephone and fax) that enjoy the protection of technological neutrality, and "new" technologies, the presence of which have the perceived potential to threaten civilization.[3] Over the past two years, countless attempts have been made to demonise a wide spectrum of technologies – indeed any device or technique even tangentially associated with criminal behaviour. Renewed demands for controls on technology standards, limitations on privacy, the establishment of identity cards, the widespread installation of video surveillance cameras, expansion of data surveillance and restrictions on encryption have been greeted by an even mix of consternation and celebration.

> **"The pressure on free expression and other rights in Canada has been profound, a situation made even more fragile because of that country's lesser level of constitutional protections."**

The events of September 11 clearly highlighted the threat pathology. Venom has been directed with particular effect on secure communications, open source information and the right of privacy. Writing in the Washington Post, Dennis Pluchinsky, a senior intelligence analyst with the Diplomatic Security Service in the U.S. Department of State argued that all media (including the Internet) should be subjected to comprehensive controls so that crucial information could not be accessed by terrorists. "A skeptic would call this censorship; a patriot would call it cooperation".[4]

> **"Over the past two years, countless attempts have been made to demonise a wide spectrum of technologies - indeed any device or technique even tangentially associated with criminal behaviour."**

Attacks on open source information and free speech have rarely been subtle. In what some critics regarded as a transparent broadside on the Internet, former chief of operations at the FBI Buck Revell warned the Congressional Committee on International Relations "The Internet now allows even small or regional terrorist groups to have a worldwide C3I (Command, Control,

Communication and Intelligence) system, and propaganda dissemination capability".[5]

Anyone in the business of promoting open source, strong encryption, freeware or privacy services is accustomed to sustained attack from government agencies. But without care, in the current climate, such elements as privacy and security design could effectively be nationalised through over-zealous regulation[6].

> **"Without care, in the current climate, such elements as privacy and security design could effectively be nationalised through over-zealous regulation."**

The zeal to limit rights involves dangerous elements of opportunism. Consider the recent U.S. state government proposals to clamp down on the public's access to government documents and meetings, ostensibly driven by concerns that terrorists could use the information. States that have passed or are considering measures to limit public access include Michigan, Florida, Minnesota, Missouri, Idaho, Maryland, Massachusetts, Tennessee and Washington.[7] While there may be some limited justification for conditional restraints, it is also true that the many of these states had consistently attempted such restrictions prior to September 11. Such measures have thrown into reverse the trend to improve public access to government through electronic means.

> **"Another remarkable change has been the increase in exceptions to Freedom of Information and related acts; further altering the relationship between individuals and governments."**

US legislative initiatives have changed the international regulatory landscape in a number of ways, particularly from the perspective of surveillance and due process rights. The United Kingdom introduced legislation regarding the retention of traffic data; while the U.S. government reduced oversight for access to communications and traffic data. Another remarkable change has been the increase in exceptions to Freedom of Information and related acts; further altering the relationship between individuals and governments. Canada attempted to include greater powers for law enforcement and national security agencies while ensuring that oversight to exempt data banks would be removed from the Information and Privacy Commissioners.

Footnotes

[1]Simon Davies, "September 11 one year on: where are we now", in Communications of the ACM, September 2002,

[2]"The "E" in terrorism", Christian Science Monitor, September 20, 2001

[3]Simon Davies and Ian Brown; "The new corporate threat to freedom of expression". Third UNESCO Congress on Ethical, Legal and Societal Challenges of Cyberspace, Paris, November 2000

[4]Dennis Pluchinsky "They Heard It All Here, And That's the Trouble", Washington Post, June 16, 2002; Page B03

[5]Statement of Oliver Revell to the Committee on International Relations, US House of Representatives, Hearing on "Al Qaeda and the Global Reach of Terrorism", October 3, 2001

[6]Simon Davies, CACM, ibid

[7]Associated Press report, published in the New York Times, February 5, 2002

Canada

The *Constitution* guarantees to everyone the fundamental freedom of "thought, belief, opinion and expression, including freedom of the press and other media of communication."[1]

The Supreme Court has recognized freedom of expression as lying at the heart of a free and democratic society and inherent to the Canadian system of government[2] and has given "expression" an exceptionally wide definition. However, freedom of expression is not an absolute right, but is subject to "such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society".[3] In fact, the Supreme Court has demonstrated considerable tolerance for laws that limit freedom of expression in the name of protecting minority interests, such as those prohibiting hate speech[4] and pornography.[5] Similarly, protection of reputation has sometimes prevailed over expression.[6] On the other hand, the courts have subjected laws constraining political speech during elections to close scrutiny[7] and have generally interpreted laws relating to the reporting of judicial proceedings in favour of the media.[8] With respect to commercial speech, the Supreme Court has insisted upon a relatively high level of proof that legal restraints are required to achieve state objectives.[9]

Although s. 8 of the *Charter* guarantees the "right to be secure against unreasonable search and seizure," and s. 7 guarantees the "right to life, liberty and the security of the person and the right not to be deprived thereof except in accordance with the principles of fundamental justice" unlike 'freedom of expression', there is no general constitutional right to privacy. Nor is there a constitutional right to freedom of information. Both the federal and most provincial governments have enacted comprehensive privacy and freedom of information legislation for the public sector. Corresponding private-sector privacy and freedom of information legislation is already enacted at the federal level and in the province of Québec, and will be in force in all other provinces and territories by January 1, 2004.[10]

Anti-terrorism and cybercrime

In response to the events of September 11, 2001, the federal government enacted omnibus anti-terrorism legislation.[11] The amendments facilitate enhanced use of electronic surveillance against terrorist groups, allow law enforcement to invoke judicially-supervised investigative hearings to compel disclosure of information related to terrorism; and, allow for the suppression of information in the national interest during judicial proceedings.[12] A bill recently introduced in Parliament would grant courts the power, on reasonable belief that a subscriber has committed an offence, to compel Internet service providers (ISPs) to produce or prepare records relating to that subscriber.[13]

As part of its anti-terrorism package, Canada also announced it would ratify the Council of Europe's *Convention on Cyber-crime*.[14] In August 2002, the federal government proposed to expand investigative powers for law enforcement, most of which would be exercised under a lower judicial standard compared to that now required to obtain search and seizure warrants or authorizations to engage in electronic surveillance. In addition, the proposal would require that ISPs make their networks wiretap compliant; introduce mechanisms to provide subscriber information to law enforcement on request; and, would create new criminal offences for virus production and dissemination.[15] These proposals have been roundly criticized by privacy commissioners, civil society advocates, and industry groups across the country as being both unnecessary and an overbroad invasion of privacy and freedom of expression rights.[16]

In 2002, the federal government amended the *Criminal Code* to provide an explicit "notice and takedown" order for the removal of child pornography or other data which makes it possible to access child pornography.[17] In 2003, a bill was introduced to criminalize electronic voyeurism and expand the "notice and takedown" order to include "voyeuristic recordings".[18] The latter bill is not yet in force.

In 2002, a Prince Edward Island court found that a proposed lottery scheme, based in the province but conducted globally over the Internet, would be illegal.[19]

In June 2002, the British Columbia Securities Commission ruled that a British Columbia resident was guilty of manipulating the price of five companies by posting hundreds of false rumors on stock chat sites.[20] The resident faces a lifetime ban from securities trading and up to C$100,000 in penalties.[21]

In December 2002, an Ontario man was convicted and fined C$100,000 for offering staged 'snuff films' on his Web site. The jury found the films had "no artistic or literary merit".[22] The prosecution is the first of its kind in Canada.

Human Rights

In 2002, the Canadian Human Rights Tribunal ordered the Canadian operator of a California-based Web site to cease and desist publication on the grounds that the content was in violation of the *Human Rights Act*[23] and would likely expose

Jews to hatred or contempt.[24] An identical order was made against British Columbia operators of a Web site whose content associated or equated homosexuality with pedophilia, bestiality and the sexual predation of children.[25] In May 2003, the Tribunal issued a cease-and-desist order against a British Columbia operator of a Web site deemed anti-Semitic.[26]

The Tribunal has taken creative steps to enforce its cease-and-desist orders by addressing aspects of extra-territoriality[27] and Internet archiving.[28]

Political speech

The *Canada Elections Act* prohibits anonymous political advertising.[29] In May 1997, the federal elections watchdog gave notice to an Ottawa operator of a political Web site that he was in violation of the law for failing to identify the sponsor of the site. He was eventually forced to remove the site under threat of fine or imprisonment, but it was immediately mirrored on other servers around the world.[30]

The *Act* bans political advertising in the 20 hour period preceding the closing of polls, but exempts any message "transmitted to the public on… the Internet before the blackout period… and not changed during that period".[31] In 2001, an Alberta court found the blackout provision violated the right to freedom of expression, but was saved by the reasonableness provision of the *Constitution*.[32] On appeal, the finding was overturned because the law did not distinguish between issue advocacy and partisan advocacy. The court found that this failure represented a disproportionate, total ban on expression and precluded citizens from meaningful expression.[33]

The *Act* prohibits premature communication of polling results prior to the close of all polling stations.[34] In September 2000, a retired teacher was charged with violating this provision when he posted to a Scottish Web site the results of a Nova Scotia by-election before the polls closed in a simultaneous by-election held in British Columbia. Although the charges were eventually thrown out on a technicality, the incident spurred another individual to post polling results gleaned from Atlantic Canada to a Web site during the 2001 general election: again, before the polls had closed in British Columbia.[35] In April 2003, the second individual was fined C$1000.[36] The court found that the prohibition violated constitutional guarantees of freedom of expresion, but that it was a reasonable limitation.

Court proceedings

Canadian law prohibits the reporting of some aspects of court proceedings. For example, Parliament has legislated restrictions on the publication of the identity of a complainant in sexual offences,[37] restricted the publication of evidence at a preliminary inquiry,[38] and evidence given at a show cause hearing.[39] In addition to these statutory restrictions, a court has the power to restrict publication of any part of a proceeding it deems necessary to protect an accused's rights to a fair trial."[40]

In 1993, an Ontario couple were charged with the abduction, rape and murder of two teenage girls. The wife was tried first and, to protect her co-accused husband' rights to a fair trial, the court issued a time-limited publication ban on most aspects of the her trial.[41] However, the case dealt with particularly gruesome facts and engendered terrific public interest at a time when the Internet was becoming a mainstream information and communication medium. Although Canadian media outlets were subject to the ban and foreign media had been excluded from the courtroom altogether, details of the trial were regularly leaked to foreign media outlets and Web sites.

Since then, court-ordered publication bans and the Internet have continued to collide. In 2001, details from the preliminary hearing of the Air India bombing were posted to an Internet Web site despite a publication ban imposed by the court.[42] In April 2003, shortly after the start of the preliminary hearings in Canada's largest ever serial murder case, defence counsel alleged violations by both U.S. and Canadian media of the court-ordered publication ban. In response, the judge threatened to bar all foreign media from covering the trial and specifically noted that publishing prohibited information on Internet sites would constitute a violation.[43]

In July 2003, the author of two controversial books on the abovementioned murder trial was arrested, had his computer seized and his Web site shut down for violating a court order to suppress materials relating to the trial. The author had posted photographs, videotapes, and interviews from the case to the Internet. The executive director of Canadian Journalists for Free Expression said his group viewed the arrest with suspicion.[44]

Blocking and filtering

There are no known instances of government attempts to block or filter certain Web sites. Nor are there public initiatives at either the federal or provincial level to force public libraries to adopt filtering software; the decision is left up to individual libraries. An informal sampling conducted by the CBC Marketplace television program indicates that even of libraries that do operate filters, most also provide unfiltered Internet terminals away from children's areas of the library.[45] The Canadian Library Association has

described filtering as a "slippery slope" and has taken a strong stand against it.[46]

In 2002, the Canadian Union of Public Employees launched six grievance hearings in an effort to force the Ottawa Public Library to prevent patrons from using Internet terminals to access sexually-explicit materials, presumably by installing filtering software.[47]

Protest and parody

In January 2001, a British Columbia court found that a union's use of an employer's domain name and meta-tags did not constitute passing-off under the *Trade-marks Act*,[48] stating that "when a Web site is used for expression in a labour relations dispute, as opposed to commercial competition, there is… a reasonable balance that must be struck between the legitimate protection of a party's intellectual property and… [freedom] of expression."[49] However, the court found that the union's use of the colour scheme, page layout, logo and other aspects of the graphic design to parody the employer's site amounted to copyright infringement because it contained no criticism nor did it mention the source and author of the site, as required by the *Copyright Act*.[50]

In 2003, a British Columbia court ordered a plaintiff in a defamation suit to 'be more specific' in a claim based on, among other things, postings made to a Web site.[51] The court found that a claim of defamation requires a greater degree of specificity than is required in most other causes of action.[52]

In July 2003, Air Canada sent a letter to the operator of a Web site critical of Air Canada CEO Robert Milton. The protest site copied the company's logo, banner and featured a photograph of an Air Canada plane.[53] An Air Canada representative stressed that the company did not object to the criticism of its officers and directors, but only to the unauthorized use of its registered trademarks.

Anonymity

In at least two cases, Ontario courts have ordered ISPs to release the names of subscribers who have allegedly made fraudulent postings in chat rooms.[54] Although the order is not granted automatically, the threshold is low. In at least two other cases Canadian courts have granted motions to compel ISPs to disclose the identity of the senders of anonymous emails to the Canadian Blood Services (CBS) agency. In both instances the correspondents had claimed that they were sexually-active gay men who had donated blood and would continue to do so in contravention of a CBS policy.[55]

In 1999, a British Columbia court granted injunctions against two Web sites on which users had posted anonymous and allegedly defamatory messages. In granting the *ex parte* motion, the judge noted that the concern for the protection of free speech was lessened because the speakers chose "to throw around accusations of the most serious kind behind the cowardly screen of an alias."[56]

In anticipation of ratifying the Council of Europe's *Convention on Cyber-crime*, the federal government has proposed introducing legislation to force ISPs to collect identifying information on their subscribers, to preserve dynamic routing information with a simple administrative order and to make their networks wiretap capable.[57] There is no requirement or proposal to require automatic data retention of all subscribers.

Unlike in some states, such as Australia, the Netherlands and Germany, there is presently no requirement for service providers to collect or maintain accurate subscriber information. The Canadian Association of Chiefs of Police has lobbied for the establishment of a national database of Internet and wireless subscribers and the requirement that service providers be held liable for collecting and maintaining accurate information on their subscribers.[58] This proposal has been met with hostility by privacy advocates and industry representatives alike.[59]

In July 2003, a British Columbia court ordered a Vancouver-based ISP to provide the identities of 30 of its subscribers to America Online, which had identified the account-holders as prolific 'spammers'.[60] Controlling spam remains on the legislative radar. In 1999, the federal government released a discussion paper on spam which concluded that the existing policy and legal framework were sufficient to address the situation.[61] Following a dramatic rise in spam, the government revisited the issue in a new discussion paper in January 2003, which raised the prospect of anti-spam legislation.[62]

Intermediary liability

There is no 'common carrier' exemption or 'safe harbour' available to Canadian Internet intermediaries as there is, for example, in the U.S. *Digital Millennium Copyright Act of 1998*.[63] ISP liability for copyright infringement must be determined on the basis of the *Copyright Act*, which exempts from liability a person whose only act in respect of the communication of a work to the public consists of providing *the means of telecommunication necessary* for another person to communicate the work.[64] In 1999, the federal Copyright Board found that ISPs were entitled to rely on this exemption.[65] On appeal, this was

affirmed, but the court found that an Internet intermediary who *caches* material does not merely provide the means necessary for another to communicate a musical work.[66] Rather, a cache operator performs an editorial function and is thus not merely a passive transmitter of data. In 2003, leave was granted to appeal this case to the Supreme Court.

Aside from issues of copyright infringement, there has been very little case law on the issue of intermediary liability in Canada.

Copyright

For a number of reasons, the tension between copyright and freedom of expression is less and criticism more muted than in the United States.[67] Unlike in the U.S., rights collectives have not yet litigated against peer-to-peer users, choosing instead to try to pin liability for the infringements of users on intermediaries.[68] In addition, the *Copyright Act* subjects manufacturers or importers of all "blank audio recording" media to a 'private copying levy': musical works copied for the private use of the person making the copy is not infringement. The provision does not exempt musical works communicated by telecommunication to the public (*i.e.* P2P file-sharing or schemes like MP3.com),[69] but the levy has nevertheless tempered Canadian copyright owners' criticism of music file-sharing. This may change as early as next year, depending on the result of the Supreme Court's consideration of Internet intermediary liability[70] and Parliament's review of the private copying levy.[71]

Canada signed the WIPO 'Internet Treaties'[72] in December, 1997, and the federal government is currently reviewing the intellectual property regime with an eye to ratifying the Treaties.[73] In May 2003, Parliament introduced a bill to retroactively extend copyright term extensions for some unpublished works.[74] Fierce public criticism prompted the government to promise to withdraw the term extension provisions, however this was subsequently reversed in June. This bill is not yet in force.

Trademarks and domain names

In January 2001, a British Columbia court found that a union's use of an employer's domain name did not constitute passing-off under the *Trade-marks Act* because although the domain name contained a registered mark, it was not identical and the context was not misleading. The court also found it significant that the site did not compete commercially with the mark holder.[75]

The Canadian, Québec and Alberta governments have all succeeded in requests for transfers of domain names registered by private parties. In all cases, the private parties had registered names for the purpose of selling or renting them and the names were found to be "confusingly similar" to actual government Web sites or agencies.[76]

In addition, there have been a number of domain dispute resolutions between private parties under the Canadian Internet Registration Authority's Domain Name Dispute Resolution Process (CDRP).[77] However, at least one critic has noted that the CDRP is not always applied predictably.[78]

Of more concern for freedom of expression than inconsistency in the CDRP, is the growing tendency of U.S. courts to apply the long-arm provision of the *Anticybersquatting Consumer Protection Act*[79] to domain name disputes between Canadian nationals merely on the basis that the domain name was registered in the United States.[80]

Footnotes

[1] *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (U.K.), 1982, c.11, s. 2(b) [*Charter*].

[2] *Reference Re Alberta Legislation*, [1938] S.C.R. 100.

[3] *Irwin Toy Ltd. v. Quebec (A.G.)*, [1989] 1 S.C.R. 927 (describes the interpretative analysis framework to be followed in freedom of expression cases. The first stage broadly interprets "expression", except for acts of violence. The second stage determines whether there has been a violation and, if so, whether it is a content-based restraint or one that merely has the effect of limiting expression. If the latter, the party claiming the protection of the *Charter* must be able to show that the activity in question promotes one of the three principles underlying freedom of expression: political debate, the marketplace of ideas, or autonomy and self-fulfillment. The final stage of the analysis places the burden on the state to justify the limit it seeks to impose as being reasonable in a free and democratic society.).

[4] *See R.* v. *Keegstra*, [1990] 3 S.C.R. 697.

[5] *See R.* v. *Butler*, [1992] 1 S.C.R. 452.

[6] *See e.g. Hill* v. *Church of Scientology*, [1995] 2 S.C.R. 1130.

[7] *See* cases on restrictions of election expenditures at *Political Speech* below.

[8] *Edmonton Journal* v. *A.G. Alberta*, [1989] 2 S.C.R. 1327, ("The importance of freedom of expression and of public access to the courts through the press reports of the evidence, arguments and the conduct of judges and judicial officers is of such paramount importance that any interference with it must be of a minimal nature.")

[9] *See e.g. Ford* v. *Quebec (A.G.)*, [1988] 2 S.C.R. 712.

[10] *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5.

[11] Bill C-36, *An Act to amend the Criminal Code, the Official Secrets Act, the Canada Evidence Act, the Proceeds of Crime (Money Laundering) Act and other Acts, and to enact measures respecting the registration of charities, in order to combat terrorism*, 1st Sess., 37th Parl., 2001 (1st reading 15 October 2001) [Bill C-36 2001]

[12] Section 104 of *Bill C-36, 2001* amends the *Privacy Act* to allow the Attorney-General to prohibit the disclosure of information 'for the purpose of protecting international relations or national defence or security.' In similar fashion, s. 103 and s. 87 amend

the *PIPEDA*, *supra* note 10, and the *Access to Information Act*, R.S. 1985, c. A-1, respectively.

[13] Bill C-46, *An Act to amend the Criminal Code (capital markets fraud and evidence-gathering)*, 2d Sess., 37th Parl., 2002, cl. 7 (1st reading 12 June 2003) (adding s. 487.012 to the *Criminal Code* 'On the basis of an ex *parte* application containing information on oath that there are reasonable grounds to believe that an offence has been or is being committed, a court may order a person, other than a person under investigation for the offence, to produce or prepare documents within the time, at the place and in the form specified to a peace officer.') [Bill C-46].

[14] Canada, News Release, "Government of Canada Introduces Anti-Terrorism Act" (15 October 2001), online: Government of Canada <http://www.sgc.gc.ca/Releases/e20011015.htm>.

[15] J. Young, "Cybercrime and Lawful Access in Canada," online: Lex Informatica <http://www.lexinformatica.org/cybercrime/> (date accessed: 27 July 2003).

[16] *See e.g.* "Surveillance law under attack" *The Globe and Mail* (8 August 2003), *see also* J. Young, "Surfing While Muslim: Privacy, Freedom of Speech and the Unintended Consequences of Cybercrime Legislation: A Critical Analysis of the Council of Europe *Convention on Cyber-crime* and the Canadian Lawful Access Proposal" (May 2003) unpublished, archived at Lex Informatica, online: http://www.lexinformatica.org/cybercrime/swm/>.

[17] Bill C-15A, *Criminal Law Amendment Act, 2001*, 1st Sess., 37th Parl., 2002, cl. 7 (assented to 4 June 2002) (amending s. 164 of the *Criminal Code* "If a judge is satisfied by information on oath that there are reasonable grounds for believing that there is…" child pornography or data which makes child pornography available…).

[18] Bill C-20, *An Act to amend the Criminal Code (protection of children and other vulnerable persons) and the Canada Evidence Act*, 2d Sess., 37th Parl., 2003, cl. 9(1) (2d reading 1 April 2003).

[19] *Reference Re Earth Future Lottery*, [2002] PESCAD 8 at paras. 10-11.

[20] *British Columbia Securities Commission* v. *Hogan* (June 19, 2002), 2002 BCSECCOM 537 (BCSC).

dissemination of misrepresentations about the five companies were acts in furtherance of his disposition of the securities of the five companies and therefore were themselves trades.

[21] Bill C-46, *supra* note 13 at cl. 2 (replacing *Criminal Code* s. 380(2) to make intent to defraud by affecting public markets an offence liable to imprisonment).

[22] *R.* v. *Smith*, [2002] O.J. No. 5018 (Sup. Ct.), *see also* K. Makin, "Man fined for obscenity over 'snuff film' Web site" *The Globe and Mail* (3 December 2002) A9.

[23] R.S.C. 1977, c. H-6, s. 13(1).

[24] *Citron et al.* v. *Zündel*, (January 2002), T460/1596 (C.H.R.D.).

[25] *Schnell* v. *Machiavelli and Associates Emprize Inc.*, (August 2002), T594/5200 (C.H.R.D.).

[26] *Warman* v. *Kyburz*, (May 2003), T726_3102 (C.H.R.D.) [*Warman*].

[27] *See* A. Humphreys, "U.S. Internet giant pulls Zundel's Web site: Canadian rights panel warned firm of hate literature" *National Post* (13 May 2003).

[28] *Warman*, *supra* note 26 at para. 86 (ordering the Canadian Human Rights Commission, a separate investigative and mediation body, to write to the operators of Archive.org requesting the removal of an archived mirror of the respondent's web site).

[29] S.C. 2000, c. 9, s. 213 (prohibition of anonymous political advertising) [*Elections Act*].

[30] A. Uncles, "Elections Canada silences a Green Party webmaster" *The Ottawa Citizen* (31 May 1997).

[31] *Elections Act*, *supra* note 29, s. 323, 324.

[32] *Harper* v. *Canada (Attorney General)*, [2001] A.J. No. 808 (Q.B.).

[33] *Harper* v. *Canada (Attorney General)*, [2002] A.J. No. 1542 at para. 154 (C.A.)

[34] *Elections Act*, *supra* note 29, s. 322.1.

[35] "Case dismissed against Internet vote-results rebel" *The Halifax Herald* (14 November 2002).

[36] *R.* v. *Bryan*, [2003] B.C.J. No. 318 at para. 13 (Prov. Ct. (Crim. Div.)).

[37] *Criminal Code of Canada*, R.S. 1985, c. C-46, s. 486(3).

[38] *Ibid.* at s. 539.

[39] *Ibid.* at s. 517.

[40] *R.* v. *Barrow* (1989), 48 C.C.C. (3d) 308 at 315 (N.S.C.A.).

[41] *R. v. Bernardo [Publication ban - Proceedings against co-accused]*, [1993] O.J. No. 2047 (Gen. Div.)

[42] R. Mattas, "Forbidden Air-India details posted on Internet Web site reveals information on suspects' bail hearing, despite ban on publication" *The Globe and Mail* (13 Feb 2001).

[43] D. Girard, "B.C. pig farmer to be tried in the deaths of 15 women" *The Toronto Star* (24 July 2003).

[44] D. Nolan, "Karla author's home raided, computers taken" *The Hamilton Spectator* (19 July 2003).

[45] R. Wright and C. Jones, "Internet Filters: Internet Filtering at selected Canadian libraries" *CBC Marketplace* (22 October 2002), online: CBC <http://www.cbc.ca/consumers/market/files/health/kids_online/policies.html> date accessed: 28 July 2003.

[46] J. Campbell, "Filtered Internet starts library down 'a slippery slope'" *The Ottawa Citizen* (28 January 2003) B1 (quoting the executive director of the CLA as stating that unfettered access to information as fundamental to an open and democratic society), *see also* R. Kantner, "Legal Issues Resulting from Internet Use in Public Libraries" (2000) 46(1) *Feliciter* 14.

[47] K. Gray, "City library becoming a 'porn palace': CUPE: Children can glimpse explicit material on library computers" *The Ottawa Citizen* (25 January 2003) D1.

[48] R.S. 1985, c. T-13.

[49] *British Columbia Automobile Assn.* v. *Office and Professional Employees' International Union, Local 378*, [2001] B.C.J. No. 151 at para. 130 (Sup. Ct.) [BCAA].

[50] *Ibid.* at para. 205.

[51] *Craig* v. *Langley Citizens' Coalition*, [2003] B.C.J. No. 141 (Sup. Ct.).

[52] *Ibid.* at para. 17.

[53] "Air Canada claims web infringement" *The Globe and Mail* (11 July 2003) B2.

[54] *Phillips Services Corp.* v. *John Doe*, (1998) Court file no. 4582/98 (Ont. Ct. (Gen. Div.)), *Irwin Toy* v. *Doe*, [2000] O.J. No. 3318 (QL).

[55] "E-mails claim gay man defied blood policy" *The Globe & Mail*, (29 July 2002). 2002), "Gay Blood Donor" *Canadian Press* (28 July 2002), "Blood services stymied in search for second gay donor through e-mails" *Canadian Press* (29 July 2002).

[56] *Henry* v. *Stockhouse Media Corp.*, [1999] B.C.J. No. 3202 (Sup. Ct.) at paras. 8-13.

[57] Canada, Dept. of Justice et al., *Lawful Access: Consultation Document* (Ottawa: Justice, 2002) [*Lawful Access*].

[58] *Ibid.* at 18.

[59] Canada, Dept. of Justice, *Summary of Submissions to the Lawful Access Consultation*, (Ottawa: Justice, 2003), online: Lex Informatica <http://www.lexinformatica.org/cybercrime/pub/la_summary.pdf> date accessed: 20 August 2003.

[60] B. Mudry, "Peer 1 accepts B.C. spam subpoena in AOL probe" *Canada Stockwatch* (10 July 2003).

[61] Industry Canada, *Internet and Bulk Unsolicited Electronic Mail (SPAM)*, (Ottawa: Industry Canada, 1999), online: <http://e-com.ic.gc.ca/English/strat/spam.html> date accessed: 5 July 2003.

[62] Industry Canada, *E-mail marketing: Consumer choices and business opportunities*, (Ottawa: Industry Canada, 2003), online: <http://e-com.ic.gc.ca/english/strat/email_marketing.html> date accessed: 5 July 2003.

[63] Pub. L. No. 105-304, § 512 (1998).

[64] R.S.C. 1985, c. C-42, s. 2.4(1)(b) [*Copyright Act*].

[65] *Re Tariff 22*, *infra* note 68 at 38 (In general, the parties who may rely on this exemption include an ISP of the person who makes the work available, persons whose servers are used as a cache or mirror, the recipient's ISP, and those parties who operate routers used in the transmission. However, the exemption may not apply to a person who has a relationship with the person who makes the musical work available so as to be acting in concert with that person, or if the person's role is not confined to that of an "intermediary.").

[66] *SOCAN* v. *CAIP et al.*, [2002] FCA 166 at para. 161, leave to appeal to S.C.C. granted [Tariff 22 Appeal].

[67] *See e.g.* J. Cohen, "Information Rights and Intellectual Freedom" in A. Vedder, ed., *Ethics and the Internet* (Antwerp: Intersentia, 2001) at 22 ("with these [safe harbour] provisions, copyright law now gives content owners new powers to silence creators of unauthorized expression, including fair use expression.").

[68] *SOCAN Statement of Royalties, Public Performance of Musical Works 1996, 1997, 1998 (Tariff 22, Internet) (Re),* (1999) 1 C.P.R. (4th) 417 (Copyright Board) [*Re Tariff 22*].

[69] *Copyright Act*, *supra* note 64, s. 80(2)(c).

[70] *SOCAN* v. *CAIP et al.*, [2002] FCA 166 at para. 161, leave to appeal to S.C.C. granted.

[71] *See* Canada, Industry Canada, *Supporting Culture And Innovation: Report on the Provisions and Operation of the Copyright Act* (Ottawa: Intellectual Property Policy Directorate, 2002) [Section 92 Report].

[72] *WIPO Copyright Treaty*, Dec. 20, 1996, 36 I.L.M. 65, WIPO Publ. No. 226(E), *WIPO Performances and Phonograms Treaty*, Dec. 20, 1996, 36 I.L.M. 76, WIPO Publ. No. 227(E).

[73] Section 92 Report, *supra* note 71 at 42ff.

[74] Bill C-36, *An Act to establish the Library and Archives of Canada, to amend the Copyright Act and to amend certain Acts in consequence*, 2d Sess., 37th Parl., 2003 (first reading 8 May 2003) [Bill C-36 2003].

[75] *BCAA*, *supra* note 49 at paras. 123-126.

[76] *See e.g. Government of Canada* v. *David Bedford a.k.a. DomainBaron.com* (2001), WIPO Case D2001-0470, (UDRP), *Gouvernement du Québec* c. *Peter McCann* (2002), WIPO Case D2002-1010, (UDRP), *Government of Canada* v. *David Bedford a.k.a. Abundance Computer Consulting* (2003), CIRA Case 00011 (CIRA), *Government of Alberta* v. *Advantico Internet Solutions, Inc.* (2003), 00012 (CIRA).

[77] *See e.g. Red Robin International* v. *Greg Tieu* (2002), CIRA Case 00001 (CIRA), *Canadian Broadcasting Corporation* v. *William Quon* (2002), CIRA Case 00006 (CIRA), *Great Pacific Industries, Inc.* v. *Ghalib Dhalia* (2003), CIRA Case 00009 (CIRA).

[78] M. Geist, "Fairness demands review of domain-name policy" *The Toronto Star* (11 August 2003), *see e.g. Air Products Canada* v. *Index Quebec, Inc.* (2002), CIRA Case 00007 (CIRA) (domain name "airproducts.ca" not deemed confusingly similar to name of complainant company; registration of thousands of domain names not demonstrating 'bad faith' on part of defendant).

[79] 15 U.S.C. § 1125(d). (A challenge inherent in resolving domain name disputes is that the parties will frequently reside in different jurisdictions. While the trademark holder may be able to obtain a local court order to have the domain name transferred or cancelled, enforcing the order against an *ex juris* registrant is often expensive. The ACPA addresses this by granting trademark holders the right to file an *in rem* action against the domain name itself, rather than an *in personam* suit against the registrant).

[80] *A.E. Heathmount* v. *Technodome.com*, 106 F.Supp. 2d 860 (E.D. Va. 2000), *see also* M. Geist, "U.S extends its hegemony over the Net" *The Toronto Star* (9 June 2003).

United States

The US has some of the world's strongest protections for civil rights. It has progressive constitutional protections and laws that promote freedom of speech, freedom of information and privacy. It was the birthplace and the loudest cheerleader of the Internet for many years. However, it has also been a leader at attempting to place controls on the Internet in the name of protecting children and corporations. The 11 September attacks gave the US government the opportunity to adopt law enforcement policies that had failed to win public support in the 1990s, such as enabling law enforcement to monitor Internet traffic in detail and limiting access to certain types of public information.

More than half of all Americans are online and 33.6 million (about 21 percent) have high-speed connections. The Internet is a vital means of communication in the United States, and became so much more quickly than in other countries, in part due to the high penetration of personal computers. One consequence is that there are relatively few Internet cafes; public access to the Internet in the US tends to be limited to schools and libraries.

The First Amendment of the US Constitution provides for the strongest protection of free speech of any Constitution in the world. Even with it, the US Congress and the states have enacted a number of laws mandating censorship of the Internet. Most of these laws have been rejected by the courts.

In 1996, the US Congress adopted the Communications Decency Act. It created criminal penalties for the "knowing" transmission of "any comment, request, suggestion, proposal, image, or other communication which is obscene or indecent," or "patently offensive messages" to any recipient under 18 years of age. The CDA was struck down by the Supreme Court in June 1997 which noted that, "the CDA… threatens to torch a large segment of the Internet community."

In 1998, Congress adopted the Child Online Protection Act that criminalizes making available information that would be "harmful to minors". It was struck down by an Appeals Court in 2000 because it overly threatened adult free speech. The Supreme Court in May 2002 sent the case back to the appeals court that ruled again in March 2003 that the law was unconstitutional. In July 2003, the Bush Administration announced that it was asking the Supreme Court to review the decision again.

In June 2003, a sharply divided Supreme Court upheld the Children's Internet Protection Act (CIPA). CIPA, which passed in April 2001, requires public schools and libraries to use filtering software on all computers used to access the Internet as a condition of federal funding under the E-Rate program. CIPA is intended to protect children by preventing them from accessing material such as pornography, bomb-making recipes, and hate speech online. The Court ruled that because it was tied to a government subsidy, the government could attach conditions. However, the court also found that the blocking must be turned off for any adults who wished to have access to the Internet and sites that might be blocked from children.

Requiring the use of filtering software in those locations as a condition of funding is a particular issue in the US; the censorship imposed by such software falls disproportionately on disadvantaged sectors of society. However, the publishers of filtering software are typically secretive about the specific sites that they block, many of which have been determined by outside sources to be overbroad and subject to political biases. Filtering companies have even gone so far as to sue to stop those who reverse-engineer the software in order to analyse its workings. The decisions about what to block embedded in this type of software are wholly taken by the companies that produce the software; they are not open to public policy debate.

The September 11 attacks led to unprecedented new powers for the government to conduct surveillance within the US. In October 2001, Congress, with little debate and under strong pressure from the Bush Administration enacted the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act, a hodgepodge of new powers that had been previously rejected by Congress. It expands the use of wiretaps and "pen registers" including authorizing the use of the controversial "Carnivore" Internet surveillance device. "Sneak and Peek" searches can be done without notifying the target. Libraries, bookstores, businesses and other organizations can be required to provide records of the customers. Some of the provisions are subject to a sunset clause. The Homeland Security Act enacted in 2002 created the Department of Homeland Security a super-agency made of 160,000 employees (one out of every 12 federal employees) who previously worked for other departments. A late amendment to the Act, the Cyber Security Enhancement Act of 2002 expands penalties for computer crimes, allows ISPs to provide government officials with access to user's communications in "good faith" if they believe there is an emergency and exempts critical

infrastructure information from the Freedom of Information Act.

Freedom of information has suffered other setbacks under the Bush Adminsitration. The September 11 attacks provided justification for the withdrawal of a number of types of government information on the web. The Bush Administration had already been accused of being the most secretive government in many decades. On October 12, 2001 Attorney General John Ashcroft issued a policy memorandum on the Freedom of Information Act that encourages government officials to deny access to information. At the same time, other "sensitive" information such as the locations of nuclear power plants, chemical hazard risk management plans, pipeline maps, and reports related to other hazards were removed from government agency Web sites on the grounds of national security.

A backlash to the Bush administration's policies is building, as conservatives and liberals criticize the wide scope of the laws and their use by the Department of Justice. Many local jurisdictions have enacted resolutions rejecting the powers and bills are now being introduced in Congress to restrict their use.

Censorship in the name of protecting intellectual property and other corporate rights is also increasing. The 1998 Digital Millennium Copyright Act, passed after heavy lobbying from the entertainment industry, contains clauses that criminalise circumvention of technology used to protect copyright. The DMCA gives the entertainment industry extraordinary latitude to undermine traditional limits to copyright such as fair use and the first sale doctrine. Many states are now considering adopted similar laws on the local level.

In 2001, the first prosecution under the act was made when Dmitry Sklyarov, a visiting Russian programmer was arrested in Las Vegas. Sklyarov and his company, Elcomsoft, had developed a program designed to remove the digital rights management restrictions applied to Adobe eBooks so that users could make back-up copies or use screen-access readers. In December 2002 a jury found Elcomsoft not guilty.

In 2002, Internet search engine Google was forced by the Church of Scientology (which has been one of the most active organizations worldwide using copyright laws to censor criticism) to remove links to criticism sites or face crushing lawsuits. The DCMA has also been used to threaten Princeton researcher Edward Felten, who was forced to withdraw a paper from a conference explaining the inner workings of a digital rights management system; against users posting DeCSS, which makes it possible to view DVDs on a Linux system and bypass their copy protection; as well as to a company making remotely controlled garage doors, which cited it in an attempt to block a competitor from selling compatible universal products.

The DMCA allows intellectual property holders to demand information about users from ISPs without a court order. The Recording Industry Association of America, which had previously pursued file-sharing networks such as Napster and Morpheus on the grounds of copyright infringement, has said it wants to charge ISPs that give consumers access to free music swapping sites, and in mid 2003 began issuing hundreds of subpoenas to individual Internet users (or their parents or roommates) hosting files for download over P2P networks after getting identifying information from their ISPs. Verizon, a leading ISPs and telecommunications company challenged the use of the subpoenas issued by the RIAA to obtain the name and details of a subscriber it alleged was violating copyright by making hundreds of songs available online. A trial court ruled against Verizon in April 2003. Some schools, including MIT, are resisting the release of student information.

Also included in the DMCA was the "Sonny Bono" Copyright Term Extension Act which lengthened the term of copyright protection to life plus 70 years, effectively ensuring that corporately owned content will stay out of the public domain for at least a century. In 2001, Eric Eldred, who was required to take down from his Web site formerly public domain works that under the CTEA had gone back into copyright, sued the government on the grounds that the CTEA was unconstitutional. In January 2003 the Supreme Court upheld the CTEA, but noted the importance of fair use and the public domain.

Censorship through copyright restrictions has also been an issue in the software industry, where end-user licence agreements (EULAs) have begun imposing a wide range of conditions, such as banning reverse-engineering or requiring permission for users to write and publish reviews and criticisms of the software. In early 2003, a New York court ruled that a no-reviews clause in a Network Associates EULA was "deceptive". The open-source movement to create software that is both free and freely modifiable has gained ground in part because of such practices. Revisions to the Uniform Commercial Code that governs interstate commerce, the Uniform Computer Information Transactions Act (UCITA) have been hotly debated, largely because UCITA's would impose on digitally encoded books, movies, and music the type of restrictions common in the software

industry. UCITA has been controversial and many of its original sponsors have withdrawn their support for it after only two states adopted it.

References

American Civil Liberties Union
http://www.aclu.org/

Electronic Privacy Information Center
http://www.epic.org

Electronic Frontier Foundation
http://www.eff.org

American Library Association Filters Page
http://www.ala.org/alaorg/oif/
filtersandfiltering.html

OMBWatch, Access to Government Information
Post September 11th
http://www.ombwatch.org/article/articleview/
213/1/104/

Peacefire (analysis of blocking software)
http://www.peacefire.org

DMCA
http://www.eff.org/IP/DMCA/

PATRIOT Act
http://www.epic.org/privacy/terrorism/usapatriot/

Chilling Effects
http://chillingeffects.org/

Cases
CDA Page
http://www.epic.org/free_speech/cda/

CIPA
http://www.ala.org/cipa/

COPA Case
http://www.epic.org/free_speech/copa/

Eldred vs. Ashcroft
http://www.eldred.cc

Addendum
Building Big Brother

This material is extracted from an annual publication produced by the US Electronic Privacy Information Center (EPIC) and Privacy International. Now in its sixth edition, the Privacy & Human Rights Report has become the most comprehensive global analysis in the field. It outlines legal protections for privacy, and summarises important issues and events relating to privacy and surveillance. This summary provides a context to better understand the implementation of restrictions on free speech in the electronic realm.

Legal and Technical Standards for Surveillance:

In the past fifteen years, the United States government has led a worldwide effort to limit individual privacy and enhance the capability of its police and intelligence services to eavesdrop on personal conversations. This campaign had two strategies. The first is to promote laws that make it mandatory for all companies that develop digital telephone switches, cellular and satellite phones and all developing communication technologies to build in surveillance capabilities; the second is to seek limits on the development and dissemination of products, both in hardware and software, that provide encryption, a technique that allows people to scramble their communications and files to prevent others from reading them.[1]

Law enforcement agencies have traditionally worked closely with telecommunications companies to formulate arrangements that would make phone systems "wiretap friendly." These agreements range from allowing police physical access to telephone exchanges, to installing equipment to automate the interception. Because most telecommunications operators were either monopolies or operated by government telecommunications agencies, this process was generally hidden from public view.

Following deregulation and new entries into telecommunications in the United States in the early 1990s, law enforcement agencies, led by the FBI, began demanding that all current and future telecommunications systems be designed to ensure that they would be able to conduct wiretaps. After several years of lobbying, the United States Congress approved the Communications Assistance for Law Enforcement Act (CALEA) in 1994.[2] The act sets out legal requirements for telecommunications providers and equipment manufacturers on the surveillance capabilities that must be built into all telephone systems used in the United States. In 1999, at the request of the Federal Bureau of Investigation, an order was issued under CALEA requiring carriers to make available the physical location of the antenna tower that a mobile phone uses to connect at the beginning and end of a call.[3]

In the United Kingdom the Regulation of Investigatory Powers Act 2000 requires that telecommunications operators maintain a "reasonable interception capability" in their systems and be able to provide on notice certain "traffic data."[4] It also imposes on obligation on third parties to hand over encryption keys. These requirements were recently clarified in the Regulation of Investigatory Powers (Maintenance of Interception Capability) Order 2002.

In the Netherlands, a new Telecommunications Act was approved in December 1998 that required that Internet Service Providers have the capability by August 2000 to intercept all traffic with a court order and maintain users logs for three months.[5] The law was enacted after XS4ALL, a Dutch ISP, refused to conduct a broad wiretap of electronic communications of one of its subscribers. In New Zealand, the Telecommunications (Residual Powers) Act 1987 requires network operators to assist in the operation of a call data warrant (equivalent to the United States trap and trace or pen register warrant)._[6] An obligation to assist in the operation of a full interception warrant is now also being considered in New Zealand. The Telecommunications (Interception Capabilities) Bill currently being drafted by the Government would require all Internet Service Providers and telephone companies to upgrade their systems so that they are able to assist the police and intelligence agencies intercept communications. It would also require a telecommunications operator to decrypt the communications of a customer if that operator had provided the encryption facility.[7]

In January 2002, a new Law on the surveillance of mail and telecommunications entered into force in Switzerland, requiring ISPs to take all necessary measures to allow for interception.[8] In contrast, the Austrian Federal Constitutional Court held, in a decision[9] in February 2003, that the law compelling telecommunications service providers to implement wiretapping measures at their own expense is unconstitutional.[10] Most recently, Poland and New Zealand have been reported as proposing and adopting new laws requiring ISPs to monitor and record communications transactions.

International cooperation played a significant role in the development of these standards.In 1993, the FBI began hosting meetings at its research facility in Quantico, Virginia called the "International

Law Enforcement Telecommunications Seminar" (ILETS). The meetings included representatives from Canada, Hong Kong, Australia and the European Union. At these meetings, an international technical standard for surveillance, based on the FBI's CALEA demands, was adopted as the "International Requirements for Interception." In January 1995, the Council of the European Union approved a secret resolution adopting the ILETS standards.[11] Following this, many countries adopted the resolution into their domestic laws without revealing the role of the FBI in developing the standard. Following the adoption, the European Union and the United States offered a Memorandum of Understanding (MOU) for other countries to sign to commit to the standards. Several countries including Canada and Australia immediately signed the MOU. Others were encouraged to adopt the standards to ensure trade. International standards organizations, including the International Telecommunications Union (ITU) and the European Telecommunication Standardisation Institute (ETSI), were then successfully approached to adopt the standards.

The ILETS group continued to meet. Several committees were formed and developed a more detailed standard extending the scope of the interception standards. The new standards were designed to apply to a wide range of communications technologies, including the Internet and satellite communications. It also set more detailed criteria for surveillance across all technologies. The result was a 42-page document called ENFOPOL 98 (the European Union designation for documents created by the European Uni Police Cooperation Working Group).[12]

In 1998….(a) new document, now called ENFOPOL 19, expanded the type of surveillance to include "IP address (electronic address assigned to a party connected to the Internet), credit card number and E-mail address."[13]

Internet Surveillance: Black Boxes and Key Loggers

A related development has been the use of "black boxes" on ISP networks to monitor user traffic. The actual workings of these black boxes are unknown to the public. What little information has been made public reveals that many of the systems are based on "packet sniffers" typically employed by computer network operators for security and maintenance purposes. These are specialized software programs running in a computer that is hooked into the network at a location where it can monitor traffic flowing in and out of systems. These sniffers can monitor the entire data stream searching for key words, phrases or strings such as net addresses or e-mail accounts. It can then record or retransmit for further review anything that fits its search criteria. In many of the systems, the boxes are connected to government agencies by high-speed connections.

In some countries, there have been laws or decrees enacted to require the systems to build in these boxes. Russia was the first country where this requirement was made public, and according to Russian computer experts, the United States government advised them on implementation. In 1998, the Russian Federal Security Service (FSB) issued a decree on the System for Operational Research Actions on the Documentary Telecommunication Networks (SORM-2) that would require ISPs to install surveillance devices and high-speed links to the FSB which would allow the FSB direct access to the communications of Internet users without a warrant._[14] ISPs are required to pay for the costs of installing and maintaining the devices. When an ISP based in Volgograd challenged FSB's demand to install the system, the local FSB and Ministry of Communication attempted to have its license revoked. The agencies were forced to back off after the ISP challenged the decision in court. In a separate case, the Supreme Court ruled in May 2000 that SORM-2 was not a valid ministerial act because it failed several procedural requirements.

Following the Russian lead, in September 1999, Ukrainian President Leonid Kuchma proposed requiring that ISPs install surveillance devices on their systems based on the Russian SORM system. The rules and a subsequent bill were attacked by the Parliament and withdrawn. However, in August 1999, the security service visited several the large ISPs who were reported to have installed the boxes.

In the Netherlands, following the passage of the 1998 Telecommunications Act (see above), the Dutch Forensics Institute[15] developed a "black-box" for ISPs to install on their networks. The black box would be under control of the ISP and turned on after receiving a court order. The box would look at authentication traffic of the person to wiretap and divert the person's traffic to law enforcement if the person is online. Due to the inability of ISPs to adopt the requirements of the law, however, its implementation has been delayed.

In China, a system know as the "Great Firewall" routes all international connections through proxy servers at official gateways, where Ministry for Public Security (MPS) officials identify individual users and content, define rights, and carefully monitor network traffic into and out of the country. At a 2001 security industry conference, the government announced an ambitious successor

project known as "Golden Shield." Rather than relying solely on a national intranet, separated from the global Internet by a massive firewall, China will now build surveillance intelligence into the network, allowing it to "see," "hear" and "think."[16] Content-filtration will shift from the national level to millions of digital information and communications devices in public places and people's homes.[17] The technology behind Golden Shield is incredibly complex and is based on research developed largely by Western technology firms, including Nortel Networks, Sun Microsystems and others. The Golden Shield efforts do not signal an abandonment of other avenues of access and content control. For example, details are only beginning to emerge about a new "black box" device, derived from technology previously used in airline cockpit data recorders, and broadly similar to the Carnivore system. Chinese Internet police would use the black box technology to monitor dissidents and collect evidence on illegal activities.[18]

New methods of surveillance, and in particular those capable of circumventing encryption, are also being developed. One such technological device is a "key logger" system. A key logger system records the keystrokes an individual enters on a computer's keyboard. Keystroke loggers can be employed to capture every key pressed on a computer keyboard, including information that is typed and then deleted. Such devices can be manually placed by law enforcement agents on a suspect's computer, or installed "remotely" by placing a virus on the suspect's computer that will disclose private encryption keys.

The question of such surreptitious police decryption methods arose in the case of *United States v Scarfo*.[19] There, the FBI manually installed a key logger device on the defendant's computer in order to capture his PGP encryption password. Once they discovered the password, the files were decrypted, and incriminatory evidence was found. In December 2001, the United States FBI confirmed the existence of a similar technique called "Magic Lantern."[20] This device would reportedly allow the agency to plant a Trojan horse keystroke logger on a target's computer by sending a computer virus over the Internet; rather than require physical access to the computer as is now the case. The new Danish Anti-Terrorism law, enacted in June 2002, appears to give law enforcement the power to secretly install this kind of snooping software on the computers of criminal suspects.[21]

Retention of Traffic and Location Data

On May 30, 2002, the European Parliament voted on the new European Union Electronic Communications and Privacy Directive.[22] In a remarkable reversal of their original opposition to data retention, the members voted to allow each European Union government to enact laws to retain the traffic and location data of all people using mobile phones, SMS, landline telephones, faxes, e-mails, chatrooms, the Internet, or any other electronic communication devices, to communicate. The new Directive reverses the 1997 Telecommunications Privacy Directive by explicitly allowing European Union countries to compel Internet service providers and telecommunications companies to record, index, and store their subscribers' communications data.[23] The data that can be retained includes all data generated by the conveyance of communications on an electronic communications network ("traffic data") as well as the data indicating the geographic position of a mobile phone user ("location data").[24] The contents of communications are not covered by the data retention measures. These requirements can be implemented for purposes varying from national security to criminal investigations and prevention, and prosecution of criminal offences, all without specific judicial authorization.

Although this data retention provision is supposed to constitute an exception to the general regime of data protection established by the directive, the ability of governments to compel Internet service providers and telecommunications companies to store all data about all of their subscribers can hardly be construed as an exception to be narrowly interpreted. The practical result is that all users of new communications technologies are now considered worthy of scrutiny and surveillance in a generalized and preventive fashion for periods of time that States' legislatures or governments have the discretion to determine. Furthermore, because of the cross-border nature of Internet communications, this Directive is likely to have negative repercussions for citizens of other countries. There is a significant risk that non-European Union law enforcement agencies will seek data held in Europe that it can not obtain at home, either because it was not retained or because their national law would not permit this kind of access.

During the debates on the Directive, many members of the European Parliament, and the European Union privacy commissioners consistently opposed data retention, arguing that, these policies are in contravention of data protection practices of deletion of data once it is no longer required for the purpose for which it was collected; and also in contravention of proportionality principles in accordance with constitutional laws and jurisprudence. Similarly, the Global Internet Liberty Campaign, a coalition of 60 civil liberties groups organized a campaign and drafted an

open letter to oppose data retention. The letter was sent to all European Parliament members and heads of European Union institutions after more than 16,000 individuals from 73 countries endorsed it in less than a week. The letter asserted that data retention (for reasons other than billing purposes) is contrary to well-established international human rights conventions and case law.

While a few other countries have already established data retention schemes (Belgium, Denmark, France, Spain, Switzerland and the United Kingdom) the implementation phase of the Directive's data retention provision may be bumpy in other Member States. Already in the United Kingdom, after a review by a parliamentary committee, significant questions have been raised regarding the legality, invasiveness, and the financial burdens involved in data retention.[25] The Directive may be seen as being in conflict with the constitutions of some European Union countries, with respect to fundamental rights such as the presumption of innocence, the right to privacy, the secrecy of communications, or freedom of expression.[26] In Finland, because of concerns regarding freedom of speech and privacy, content retention requirements have been reduced to three weeks at most, and for Internet traffic data no retention is required.[27]

Meanwhile, the situation is uncertain in Austria, Germany, Greece, Italy, Luxembourg, Portugal, and Sweden as they consider or question the means through which they can establish retention policies.[28] In Ireland, proposals from the Department of Justice have been poorly received from the industry, the Data Protection Commissioner, the Department of Communications, and the Marine and Natural Resources.[29] Industry associations in several countries[30] and the International Chamber of Commerce have all announced their concerns with general retention laws.[31] In all, nine states have established laws so far; while ten out of fifteen EU governments favor a "harmonizing" EU measure.[32]

Footnotes

[1] *See* David Banisar & Simon Davies, "The Code War," Index on Censorship, January 1998.

[2] *See* EPIC, Wiretap, available at http://www.epic.org/privacy/wiretap/.

[3] Third Report and Order adopted by the Federal Communications Commission, In the Matter of Communications Assistance for Law Enforcement Act, CC Docket No. 97-213, FCC 99-230 (1999) (the "Order"). The Order was released on August 31, 1999. A summary of the Order was published in the Federal Register on September 24, 1999. See 64 Fed. Reg. 51710.

[4] Regulation of Investigatory Powers Act 2000, sections 12 (1) and 22 (4) respectively, available at http://www.hmso.gov.uk/acts/acts2000/20000023.htm.

[5] Telecommunications Act 1998. Rules pertaining to Telecommunications (Telecommunications Act), December 1998.

[6] Telecommunications (Residual Powers) Act 1987, section 10D.

[7] "Interception Capability - Government Decisions," New Zealand Government Executive Press Release, March 21, 2002, available at http://www.executive.govt.nz/speechaptercfm?speechralph=37658&SR=0.

[8] Loi fédérale sur la surveillance de la correspondance postale et des télécommunications, http://www.admin.ch/ch/f/rs/c780_1.html and the respective new decree http://www.admin.ch/ch/f/rs/c780_11.html.

[9] http://www.vfgh.gv.at/vfgh/presse/G37-16-02.pdf.

[10] *See* for more details http://www.epic.org/privacy/intl/austrian_vfgh-022703.html.

[11] Council Resolution of 17 January 1995 on the lawful interception of telecommunications, Official Journal of the European Communities November 4, 1996, available at http://europa.eu.int/eur-lex/en/lif/dat/1996/en_496Y1104_01.html.

[12] ENFOPOL 98, September 1998, available at http://www.heise.de/tp/deutsch/special/enfo/6326/1.html (in German). *See also* Duncan Campbell, "Special Investigation: ILETS and the ENFOPOL 98 Affair," Heise Online, April 29, 1999, available athttp://www.heise.de/tp/english/special/enfo/6398/1.html.

[13] Draft Council Resolution on the Lawful Interception of Telecommunications in Relation to New Technologies ENFOPOL 19, March 15, 1999.

[14] "Russia Prepares To Police Internet," The Moscow Times, July 29, 1998. More information in English and Russian is available from the Moscow Libertarium Forum http://www.libertarium.ru/libertarium/sorm/.

[15] *See* Dutch Forensics Institute Homepage http://www.holmes.nl/.

[16] G. Walton, China's Golden Shield: Corporations and the Development of Surveillance Technology in the People's Republic of China 9 (Rights and Democracy, 2001) available at http://serveur.ichrdd.ca/english/commdoc/publications/globalization/goldenShieldEng.html.

[17] B. Rappert, "Assessing the Technologies of Political Control" (1999) 36(6) J. of Peace Research741. The Golden Shield Project contemplates automated voice recognition through digital signal processing, distributed, network video surveillance, and content-filtration of the Internet.

[18] *See, e.g.,* L. Weijun,"China Plans to Build Internet Monitoring System," China News Daily, March 20, 2001 http://www.cnd.org/Global/01/03/20/010320-3.html.

[19] *United States v. Scarfo*, 180 F. Supp. 2d 572 (D.N.J. 2001). *See generally* EPIC's Scarfo web page http://www.epic.org/crypto/scarfo.html.

[20] Elinor Mills Abreu, "FBI Confirms 'Magic Lantern' Project Exists," Reuters, December 12, 2001.

[21] Law No. 378, June 6, 2002.

[22] Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector http://register.consilium.eu.int/pdf/en/02/st03/03636en2.pdf.

[23] Art. 15 (1), *id.*

[24] Art. 2 (b) and (c), *id.*

[25] All Party Parliamentary Internet Group, Communications Data: Report of an Inquiry by the All Party Internet Group, January 2003 http://www.apig.org.uk/APIGreport.pdf.

[26] This is, e.g., the case in Spain where the recent law allowing data retention for a year (the "LSSICE") has been challenged as being in direct opposition to the Spanish Constitution. *See generally*, EPIC's LSSI web page http://www.epic.org/privacy/intl/lssi.html.

[27] EFFi, "Finland rewrote the Internet censorship law," Press Release, February 16, 2003.

[28] "Answers to a questionnaire on traffic data retention," Council of the European Union, November, 20, 2002 http://servizi.radicalparty.org/data_retention/.

[29] Karlin Lillington, "Departments at Odds on Data Retention Bill," The Irish Times, June 27, 2003.

[30] European Competitive Telecommunications Association (ECTA"), "ECTA Statement on Data Retention in the EU," Update June 2003; *see generally* http://www.epic.org/privacy/intl/data_retention.html#industry.

[31] EICTA, ETNO, EuroISPA, ICC, Intug, and UNICE, "Common Industry Statement on Storage of Traffic Data for Law Enforcement Purposes," June 4, 2003 http://www.iccwbo.org/home/statements_rules/statements/2003/Common%20Industry%20Position%20on%20data%20retention%20final%20june%202003%20logos.pdf.

[32] Statewatch, "Majority of Governments Introducing Data Retention of Communications," January 2003, available at http://www.statewatch.org/news/2003/jan/12eudatret.htm.

Copies of the Privacy & Human Rights Report can be ordered through www.epic.org The publication is also available online at http://www.privacyinternational.org/survey/phr2003/