

Dumbing Down Democracy:Trends in Internet Regulation, Surveillance and Control in Asia*

James Gomez

Introduction: Post September 11 Online Legislation

The relationship between the growth of the Internet and attempts to control the Net can reveal much about the democratic potential the Internet offers in Asia. Observers of the Internet need to take note that the terrorist attacks of September 11, 2001 (911) have accelerated efforts to control the previously free space provided by the Internet. A slew of anti-terrorism laws have been adopted in Asia drawing upon the UN Resolution 1373, the USA Patriot Act and various European laws.

Reporters Sans Frontieres (RSF) have called 2003 “a black year” for journalists. Asia has been declared the “world’s largest prison for journalists, cyber dissidents and Internet-users”. China has the biggest number of Internet-users in prison, a total of forty-eight (48) as of 1 January 2004. Nine cyber dissidents are in prison in Vietnam, and according to Reporters Sans Frontieres, the country has set up a computer research department exclusively devoted to creating Internet surveillance software (RSF, 6 January 2004).

Reporters Sans Frontieres asserts that the Internet has suffered ‘serious battering’ since 911 and is ‘collateral damage’ in the war against terror (RSF, 5 September 2002:1). The threat of ‘terrorism’ has been used in many countries as a justification for increased security measures, including surveillance, and a reining-in of civil liberties such as freedom of expression. Following the Bali bombing in October 2002, for example, the Indonesian government was able to pass anti-terrorism regulations, increasing police powers and allowing for detention without trial, previously rejected by parliament.

The Electronic Privacy Information Center (EPIC) and Privacy International report Privacy and Human Rights 2003 identified global trends in legislative surveillance measures taken by governing authorities following 911 as: increased communications surveillance; weakened data protection regimes; increased data sharing; and increased profiling and identification.

RSF and EPIC & Privacy International are in agreement that ‘None of the above trends are necessarily new; the novelty is the speed in which these policies gained acceptance, and in many cases, became law’ (EPIC & Privacy International, 2002:27). The asserted need to track terrorists, whose primary use of the Internet appears to be the same as us ‘non-terrorists’ – for communication and discussion - increased the apparent urgency of

* Some of the ideas contained in this paper first appeared in the introduction to the book, *Asian Cyberactivism: Freedom of Expression & Media Censorship*, edited by Steven Gan, James Gomez and Uwe Johannsen (Thailand: Friedrich Naumann Foundation, 2004).

cyberspace tracking. Ultimately, 'the presumed use of the Internet by members of the terrorist commando to contact each other and prepare the operation handed a victory to advocates of very tough security measures and strict regulation of the Internet' (RSF 2, 2002:4).

While much of the above discussion centres on managing the technology in order to counter terrorist threats, it is also important to bear in mind that there are historical tensions between technology and its application in the promotion of democracy in Asia. Hence, like other past technological innovations such as the radio, television, fax machines and satellite broadcasting, the Internet represents a new type of medium that governments, as always, are keen to control.

The popular assertion often made by Internet advocates that the Internet cannot be controlled – that content control, a primary characteristic of the traditional state-media relationship, cannot be as successful or far-reaching when applied to the Internet – is indeed not true. In Asia, since 9/11, governments have tabled or passed legislation that will enable them to track and monitor content that is put online (Privacy International, 2003). Governments are giving electronic snooping powers to themselves and their various agencies to spy on others.

This raises important questions, like whether the public can be reasonably sure about the transparency of governments, even democratic ones, and about balancing the rights of the individual with the safety of the community. It also raises ethical questions on sub-contracting important state functions like surveillance to the hands of private, commercial firms - all in the name of fighting terrorism.

These developments have raised concerns at the international level that the first World Summit on the Information Society (WSIS), to be held in Geneva in the late 2003, would prompt some countries to use this 'cyber summit' to place restrictions on the Internet and other information technologies (Shashi Tharoor, 2003). In spite of the joint declaration at the December 2003 WSIS to affirm commitment to Internet freedom (WSIS, 12 December 2003), the desire of governments to extend restrictions against the Internet continues unabated as they retain the legal and legitimate right to intervene with restrictions and sanctions.

It is within this context that this paper looks at the relationship between new media and democracy in the post-9/11 period. It plots the early legislations surrounding it and shows that regimes in Asia are doing their very best to control this medium when it comes to political content even as the technology evolves. The paper concludes by arguing that such measures in several ways serve to weaken the democratic potential of the Internet.

Democracy, Freedom of Expression and New Media in Asia

Democracy in Asia has traditionally met a strong conservative reaction in the region. This is due to the aftermath of the Second World War, where re-construction and development took priority over political expression and participation. The rapid economic growth of

many Asian economies in the 1980s and the rise of an urban middle class did not result in democratic change. Instead advocates of 'Asian Values', argued that democracy and humans rights standards were cultural-specific, and defended the economic growth of the Asian economies as the outcome of the 'Asian way' of strong government, social conservatism and free market economies.

The Asian financial crisis of 1997 exposed the institutional weaknesses in the region, and heralded the space for economic and political reform. This included the emergence of civil society as holding the potential to require transparency and accountability of Asian governments. The spread of the Internet, the English language, cheaper international telephone charges and global air travel were additionally put forward as contributing to the push towards democracy (Gomez and Smith, 2003).

The expansion of freedom of expression and the decline of censorship has often been associated with the movement towards democracy. While some agree that in Asia there has been some movement towards democracy (AMIC, 2000), it is unclear whether this involves a decline of censorship and an increase in freedom of expression. With regard to the history, much of the law and methods of government control of media in the region were enacted by the colonial authorities and later adopted and refined by postcolonial regimes. Strict regulation of the media, especially with regards to political content, has been the consistent feature. Patterns of containment of freedom of expression include the use of legislation to restrict access, proscribing content, exercising influence through ownership and inducing self-censorship.

When the Internet first emerged in Asia in the early 1990s, there was hope that an open space would emerge whereby public discourse could take place without the mediation of licensing authorities, and the gate-keeping and agenda-setting of the mass media. Since, technically, individuals could communicate with each other across geographical and political boundaries without restriction, and once a text is posted on the Internet the ability to control its movement is minimal, the notion of censorship that was so strongly present in traditional media was viewed to have an uncertain future on the Internet. Many were confident that any attempt by authorities to protect data or censor information could be circumvented by choosing to re-route or taking avoidance measures. In this regard, there were expectations that freedom of expression would increase and help further democratic development in the region.

It is naïve however to expect that new media technologies alone can achieve democracy – since the crucial ingredients for establishing a full and functioning democracy are an active and politicised citizenry, a vibrant civil society and a state that is attentive to human and civil rights. Many observers and analyst forget that activism in one form or another has always been present in all societies. What authoritarian regimes do, for example in Asia, is to restrict the opportunities for activists to use the traditional methods of communications such as direct communications, pamphleteering, newspaper publishing, setting up community radio, getting access to print and broadcast media, and others. The difference with the advent of new information and communication technologies is that activists can now avail themselves with a variety of online and

mobile communications tools. They use these new tools to mobilise people for action around a cause or issue, making them cyberactivists. The tension now lies in the move by conservative regimes to make new laws and place restrictions on activists who might use such new technologies for advocacy.

Several studies meanwhile have concluded that the initial euphoria concerning the democratic potential of the Internet was misplaced. Such studies show that information technology alone cannot introduce democracy (Kalathil and Boas, 2003), hence the Internet is not necessarily a threat to authoritarian regimes. Other writers point to issues such as social engineering, de-politicisation and self-censorship as being responsible for a politically apathetic and fearful citizenry that is reluctant to use the Internet for its optimal political potential (Banerjee, 2003).

Yet it is important to note that the Internet is continually re-inventing itself and its potential to contribute towards democratic change cannot be judged prematurely. Trends arising from the Internet's inherent characteristics of collaboration and information sharing, as well as how wireless technology and the growth of 'blogging' reflect the democratic principles that led to the Internet's creation, making a case for its significance as an instrument in bringing about democratic change in Asia.

Hence, new media remains a cause for concern especially for conservative regimes, thus, attempts to control the Internet began early enough.

The beginnings of Internet censorship in Asia

In Asia, in spite of the early optimism, in reality, many governments do try to control the Internet. Pornography, hate speech and, later, gambling were early targets of web-based censorship and remain ongoing themes of concern for legislators in the region. Anti-spam legislation is an emerging area of concern.

1996 saw the Chinese authorities legislate against pornography on the Internet (State Council Order No.195, 1 February 1996). Online pornography is also prohibited under Article 5 of the Computer Information Network and Internet Security, Protection and Management Regulations (December 1997), Article 57 of the Telecommunications Regulations Of The People's Republic Of China (25 September 2000) and the Measures For Managing The Internet Information Services (25 September 2000). ASEAN representatives discussed a possible common framework and regional body to respond to pornography on the Internet (Menon, 1999). Anti-pornography measures are often complicated by varying definitions of 'pornography' and what content the censorship regulations cover. According to an Internet content rating system introduced to Hong Kong in 2001, for example, gay and lesbian websites are classified as 'harmful media', with the owner of the first and biggest gay website in the country being told to mark his site as a 'harmful site' and install filtering software to prevent youth access, or risk imprisonment. The legislation has come under heavy criticism by rights groups including Amnesty International (Amnesty International, 2002). Under the Indian Information

Technology Act 2000, Chapter XI Para 67, the government of India also declared electronic publication of pornography an offence.

More recently, governments in the region have moved to control or restrict online gambling, with some looking to supplement existing legislation prohibiting gambling with specific measures to combat online gambling. On 18 Feb 2003 prosecutors and police raided the offices of a Taiwan advertising company that had helped promote business for British Internet sports betting company Sportingbet, and a Taipei prosecutor recently indicted Dai Chi-feng for helping to transfer local gamblers to casinoluxy.com through a super link. Both actions were based on existing regulations in the Criminal Code that penalize people who instigate others to commit crimes or make profits by gathering people to engage in gambling (China Post, 2003). In 2002 China announced restrictions on Internet cafes under which customers are banned from looking at websites which offer prostitution, adult entertainment or gambling (Gambling Licenses Online, 2002). Legislators in South Korea have discussed law revisions which were to be introduced to the National Assembly sometime in 2003, preventing PC rooms and Internet cafes from providing gambling or other betting services (The Korea Times, 2003).

There have also been attempts to restrict websites that promote hatred of ethnic and religious groups. Section 4(2)g of the Singapore Internet Code of Conduct prohibits material that ‘glorifies, incites or endorses ethnic, racial or religious hatred, strife or intolerance.’ Article 5 of the Chinese Computer Information Network and Internet Security, Protection and Management Regulations, December 1997, purportedly protects ‘nationalities’. In September 2002 a website in Australia was ordered by the Federal Court to remove material that casts doubt on whether the Holocaust occurred. Judge Catherine Branson ruled that Dr Toben vilified Jewish Australians when he published documents that cast doubt over the Holocaust on the Adelaide Institute website (The Australian, 2002).

Legislation is not the only measure taken against such sites, active “blocking” (using a technical approach to deny access) of sites is also another option employed by governments. For instance in Thailand, the government filters access to Internet content by using a caching proxy server which delivers a “request denied page” instead of the one sought for by the Internet user. Thai ISPs receive official guidance from the Ministry of Information and Communications Technology via a periodic “BlockURL” message, listing domains which ISPs are supposed to look out for and block. About 1,250 sites are blocked, comprising mostly pornographic ones, a few devoted to online gaming, and one belonging to a separatist movement (Ignotus, 2004).

Apart from website, another emerging issue is spam – unsolicited email messages. Asian countries are looking towards countering it, with front runner Singapore considering specific anti-spam legislation to guard against unsolicited e-mail. Currently, spammers who do not stop their activities after their ISPs receive complaints will be ‘given the boot’. In cases like a deliberate and malicious ‘mail-bombing’ campaign, the spanner can

be charged under the Computer Misuse Act and fined up to S\$10,000 with a three-year prison sentence (Computer Times, 2003). While on the surface it would seem to most that such legislations are directed to unsolicited commercial e-mails, there are also political implications. Many NGOs and political parties use mailing lists to reach out to people in restrictive environments. Spam legislation presents governments the option to criminalise people or organisations that send out e-mail notices to individuals who claim that they had not specifically asked to be put on mailing lists. Spam messaging on mobile phones is also a growing trend in Asia as a result of the growing number of marketers using text messages to target subscribers. In Japan this is a common problem where SMS spammers generate at random the email style addresses used for text messaging. NTT DoCoMo, Japan's largest mobile phone company is taking legal action against spammers by cutting off more than 2000 lines because of spam abuse and has also sought damages in some cases (Young and Kane, 2004).

From the above issues, governments in Asia were to move quickly to focus at the political dimensions of the Internet.

Censoring Online Political Content

Authoritarian governments in Asia have from early on been interested in managing the greater political space the Internet could provide activists and democracy advocates. While it is true that governments in Asia were interested in the economic dimension of the Internet and sought to develop it (Ho et al., 2003), at the same time these very governments were also mindful of the political challenge that the Internet might pose. There are several trends that are discernable in the way they legislate against political users of the Internet.

Suppressing Political Expression

Authoritarian regimes in China and Vietnam have also implemented numerous restrictions on cyberspace, utilizing firewalls and arresting cyber-dissidents (Neumann, 2001). In this regard, Vietnam remains one of the world's most repressive countries where websites, which are considered politically and morally dangerous, including foreign news sites and those of human rights organisations, are blocked by the government. It is officially forbidden to use the Internet for political opposition, for actions against national sovereignty and security and violations of morality or the law. Violations of this regulation are often punished with imprisonment for several years. The government has plans to make Internet café owners responsible for their customer's messages and to set up a national monitoring system to ensure that cyber café users don't see "politically or morally dangerous websites" (RSF, 18 June 2003).

Several cyber-dissidents have been arrested, harassed or placed under house arrest after publishing critiques on the government and its policy or religious texts (Free Vietnam Alliance, 2002). As at January 2004, there are nine cyber dissidents in prison or under house arrest (RSF, 2004). Recent examples include Nguyen Vu Binh, a former journalist who used the Internet to criticise the government, and was arrested in an Internet café in Hanoi on 21 February 2002, after posting an article in which he criticised Vietnamese-

Chinese border agreements signed in 1999. He was held in detention without trial until he was sentenced to prison on 1 January 2004 for seven years (Index On Censorship, 2004). On 20 December 2002, cyber-dissident Nguyen Khac Toan was sentenced to 12 years in prison after he was 'found guilty of spying for e-mailing material to allegedly "reactionary" Vietnamese human rights organisations abroad'. He was arrested in a Hanoi Internet café on 8 January 2002 (IFEX, 2003).

The Chinese Communist authorities use a variety of tools to repress free expression on the Internet. These include harsh laws, stiff jail sentences, crackdowns on Internet cafés and the blocking of many 'subversive' websites, such as those of CNN, BBC and Human Rights Watch. As at December 2003, at least 48 Chinese citizens have been arrested for expressing their opinions through the Internet (IFEX, 2003). Recent examples include Kong Youping, a factory worker who was arrested on 13 December 2003 at his home for posting political articles and poems on foreign websites over the past six months (China Study Group, 2003). Another Chinese activist, He Depu, was sentenced to eight years in prison on 6 November 2003 for collaborating with the Chinese Democratic Party and posting messages on the Internet 'inciting subversion' (IFEX, 2003).

The military junta in Burma has effectively barred all Internet activity by civil society (Lintner, 2001) and is only now beginning to allow access to a limited package of approved websites, referred to as the 'Intranet'. Even then, to get a private connection to the Internet a license is required and high fees have to be paid. The initial activation costs US\$260 and a monthly fee of US\$35 for twenty hours usage has to be paid (Zaw Oo, 2004). In addition these fees are not in the local currency but in Foreign Exchange Certificates (FEC). Most of the people cannot afford these costs, thus it effectively puts it out of the reach of the general population. The number of cyber-cafes is also limited because prior approval via a licensing system is required. Again, access is limited. For instance, customers are not allowed to access free email services such as hotmail or yahoo.

Legislating against electoral use of the Internet

Singapore has seen the most comprehensive efforts by an Asian government to restrict civil society Internet space. It passed a bill in 2001 to amend the Parliamentary Elections, ahead of the last elections in 2002, drawing the boundaries on political campaigning over the Internet and barring the publication of opinion polls during a general election. Political Web sites can publish party posters and manifestos, candidate profiles, party events and positions on issues, and some moderated chats and discussion forums. On barring election surveys and exit polls, the minister said these gave the illusion of reflecting public opinion but were often based on small sample sizes, bad question design and improper sampling, which led to inaccurate and slanted results. Opposition leaders said the new law was designed to curb their efforts to reach out to the electorate via the Internet amid widespread speculation that polls would be held well before the August 2002 deadline (Wong, 2001).

In Japan, the government has taken steps to deal with the Internet as a medium for political campaign activities by applying “existing media-use legislation in the form of the Public Offices Election Law (POEL) to political content that is aimed at the electorate during official election campaign periods”. Due to the POEL and its wide range of regulations, Japan’s electoral system has been described as “one of the strictest in the world”. Its strictures constrained opposition parties from actively campaigning on the Internet during the 1998 Upper House election, but non-traditional political actors and individuals emerged in the campaign milieu, signaling an important trend. These political actors established email newsletters, bulletin-board services, chat groups, ideologically neutral portal sites, as well as “anti-candidate” websites. All of these circumvented the POEL. Unlike legislation in Singapore, the POEL did not cover email communications, giving political parties and some candidates the leeway to send email bulletins to subscribed members throughout the official election period during the 2001 Upper House election (Tkach-Kawasaki, 2003).

The high number of broadband subscribers in Korea has made the use the Internet by political parties and politicians common place. Home pages of political parties, politicians, citizen groups become especially active during election campaigns. However the law says little about the Internet and politics during campaign periods and this gave rise to some problems in the 2002 presidential campaign. In Korea, online politics has attracts a high level of citizen and civic group participation. For instance, the online media *Ohmynews*’ attempts to hold “relay interviews” with the front runners of the 2002 presidential election candidates was seen to violate Article 254 of the Elections Act because the law prohibits non-press media from having live forums just before the election campaign period (Kyu, 2003). However, this was seen as being out of synch with developments in new technology. Unlike Singapore or Japan, plans were made for positive legislation to be passed in 2003 to enable more online politicking during electoral campaign periods. Nevertheless, discrimination against online news portals remains. For instance it is well-known that government offices’ press clubs are not open to Internet reporters (Kyu, 2003)

Terrorism-related suppression and legislative measures

Attempts to regulate the Internet include legislation - some specifically targeted at the Internet as a form of communication - as well as policing and suppression activities that serve to restrict the Internet and its usage, such as surveillance, filtering, website closures and shutting down of cyber-café.

Under the label of ‘fighting terrorism’, the Pakistani government has taken measures that reduce the privacy of Internet users. Since August 2002 cyber café owners in Pakistan have to keep record of the names, connection times, numbers called and computer identities of their customers. According to the officials these records will help track down terrorists by making emails easier to trace and will help to promote security. The government announced that monitoring Internet use is necessary for Pakistan’s anti-terrorism efforts. Several websites have been blocked - an al-Qaida website and other

pages that provide 'anti-Islamic' or 'blasphemous' information (RSF, 18 June 2003; Index On Censorship, 6 August 2002).

In Bombay, Indian police are proposing a regulation requiring customers to show photo identification and give their addresses whenever they patronise any of the city's 3000 cybercafes. Cybercafe owners would have to retain these records for up to a year and show them to police on request. The proposal is to be presented in February 2004 to the Maharashtra state government (Badam, 2004). Authorities are fearful that terrorists and other criminals are taking advantage of cybercafes to communicate via email and the Internet, and the police have enlisted the help of technology experts and Internet service providers to trace emails in order to track down terrorists. Although very few countries regulate Internet cafes it certainly is an emerging trend.

Other countries such as the Philippines and Indonesia, are preparing legislation to exercise control over users of communication devices and services. The Philippines' draft Anti-terrorism Bill proposes to sanction arrests without court orders, initiate 30-day detentions without charge, among others. It would also allow the Secretary of Justice to authorize wiretaps, including those of Internet communications (Privacy International and the GreenNet Educational Trust, 2003). In order for wiretaps to work, there needs to be a certain amount of co-operation between law-enforcement agencies, telecommunications companies and Internet Service Providers, in cases where the authorities want to monitor certain user accounts. No one is sure of the extent of this cooperation (Pabico, 2003). This explains why Mobile Patrol Group (MPG) policeman traced a 17 year old who call up a police station with a bomb threat in late 2002. In this instance it was a simple case of the police hotline 116 being equipped with caller ID (SunStar Network Online, 20 October 2002). Hence, the police were able to go to the house of the teenager and traced the prankster.

After the Bali bombings in 2002, Indonesia passed an Anti-Terrorism Law under which the "security forces can intercept and examine information that is expressed, sent, received or stored electronically or with an optical device, and can detain anyone for up to three days without evidence". They can thus intercept an individual's emails and tap people's telephones (Luwarsu, 2003). Apart from law, terrorism has also led to the use of high-tech tracking devices in search and arrest of terrorist suspects. In late 2002, Indonesian police using the technology which requires only seconds to identify the location of a cell-phone were able to arrest Imam Samudra who was later confessed that he was the chief planner and coordinator of the Bali bombings (Time, 2 December 2002). It was reported again in mid-2003 that the use of similar mobile-phone tracking technology by the Indonesian police was the reason why several members of the Jemmah Islamiah easily tracked and arrested following the Bali bombings (TimeAsia, 5 May 2003). This implies even the movement of the Internet onto handheld devices can be effectively put under surveillance and traced.

Cyber security conferences

Most of the cyber security conferences in Asia deal with issues like e-commerce, virus protection, prevention of hacker attacks and a safe online business environment for companies and their customers. It can also include issues such as cyber stalking, Internet hour theft, data theft, cyber blackmail, defamation of individuals and nations, and corporate espionage. Concern over “cyber terrorism” was secondary. Since September 11 however, capacity-building to counter cyber criminals has been stepped up in the region through a series of cyber security conferences that are often supported by the United States but jointly organised with the various local partners.

One example was the early cooperation between the US Federal Bureau of Investigation (FBI) and the Indian Central Bureau of Investigation (CBI) in 2000 to fight cyber crime in India. After FBI experts trained Indian policeman to handle computer crimes, the Indian CBI then went on to set up its own Cyber crime unit. (BBC News, 23 July 2000) In February 2004, the CBI announced that they will soon begin networking with nine other Asian countries through a ‘Cyber Crime Technology Information Network System’ (CTINS) which was initiated by the National Police Agency of Japan. (newindpress.com, 2nd Feb 2004) In 2003, Pakistani ‘Federal Investigation Agency’ (FIA) officers were trained to fight cyber crime by the US Federal Bureau of Investigation. The new FIA unit, named ‘National Response Center for Cyber Crimes’ (NR3C), was set up to deal with cyber crimes in Pakistan and included plans to create a cyber security net in the country. (Crime-research.org, 11th July 2003)

Other examples of cyber security networking include a conference on strengthening international law enforcement cooperation to deal with cyber crime, held in July 2003 by the Asia Pacific Economic Cooperation (APEC) e-Security Task Group. The three primary objectives of the conference were: assisting countries to develop legal frameworks necessary to combat computer crime; to promote the development of law enforcement investigative units with the training and equipment needed to investigate and deter computer crime; and to enhance understanding and cooperation between industry and law enforcement in order to better address the threat of computer crime (APEC, 25 July 2003). A related APEC initiative is the ‘Cybersecurity tool kit’ which is to be developed jointly with several business organisations including Microsoft. This ‘kit’ will enable business to implement appropriate security measures to protect their systems. Businesses are also being encouraged to work with law enforcement agencies to investigate cyber crime (APEC, 8 Oct 2003). Such measures although aimed at cyber criminals, hackers and virus authors, can be used to prosecute pranksters and legitimate cyber activists.

Hence it is no surprise that on September 19, 2003, the Association of South East Asian Nations agreed to intensify its efforts to fight cyber crime, hackers and computer viruses. In 2004 ASEAN is setting up a framework to share information in order to respond to incidents like fast spreading viruses or other forms of “cyber crime”. Each member country will set up a “Computer emergency response team” (CERT) to coordinate the cooperation. ASEAN plans to intensify and expand the information sharing in the coming years. (reuters) These measures build on developments following 17th of May 2002 when ASEAN Member countries agreed on a work program to implement the ‘ASEAN Plan of

Action to Combat Transnational Crime'. This work program includes fighting cyber crime through online exchange of information on cyber crime activities via the ASEAN Secretariat as well as the sharing and analysis of critical intelligence information. Member countries also agreed to develop regional training programs and conferences to enhance existing capabilities in investigation intelligence, surveillance, detection and monitoring the Internet with regards to cyber crime. The Members agreed to exchange their 'best practices' in fighting cyber criminals, including ways of tracking down emails.

In February 2004, plans were announced for a new Centre for Law-enforcement Cooperation in Jakarta (Go, 5 Feb 2004). The Centre will facilitate information sharing on terrorists and their activities as well as conduct training sessions for police from Asia-Pacific countries in counter-terrorism skills (Go, 6 Feb 2004). The Centre – to be a joint Indonesian-Australian effort – was made known during a two-day conference in Bali in early February. Twenty-five countries from the region were involved in the conference with high-level US participation.

However, one underlining concern of all the above capacity building is that such expertise might be abused by certain governments especially when the proper checks and balances are not built in to protect the privacy of individuals.

Surveillance and storage of data traffic

Central to the success of control over Internet content is state ownership or regulation of ISPs, technologies that enable Internet users to be traced to their computers, and the increased inter-state pooling of surveillance information. In Asian countries cyberspace is a realm for surveillance. According to Lyon (2003), surveillance is 'focused attention on behaviours and trends of persons and of populations with a view to managing, controlling, protecting, or influencing them'. Like elsewhere, the Internet is used in Asia for repressive and illiberal purposes, and surveillance is the norm with its emergence as a 'medium for commercial, management, policing, and government activities' (Lyon, 2003).

Online surveillance is carried out by both governments and corporations. The governments of South Korea, Japan, Singapore and Hong Kong, for example, require Internet service providers to keep information on users and to help law enforcement agencies track their online activities. In Japan, the Communications Interception Law was passed in August 1999, allowing law enforcement officials access to private e-mail accounts if they were investigating certain types of crime (Williams, 2000). The Communications Authority of Thailand (CAT) by law has minimum 32 per cent share in all privately-owned ISPs. In addition the National Information Technology Committee (NITC) has ordered ISPs to retain connection data about their customers for at least three months. The purpose: to enable prosecutors to take action against those who log on to undersirable websites and to facilitate government authorities to block such sites. (Reporters Without Borders, 2002)

Similarly, handheld devices such as mobile phones are not exempt from such surveillance. In Singapore, the perpetrator of an unintentional bomb hoax via a mobile phone's short messaging system, or SMS, was traced within two weeks of the incident. This was done by the police with the cooperation of all three telecommunications companies – Starhub, M1 and SingTel. All of them store SMS messages in their servers or databases, for periods of time ranging from two days to a few weeks, before they are deleted (The New Paper, 2002, 2004). The police have powers to compel telecommunications companies to hand over information in their databases (The New Paper, 2002), and under the Telecommunications Act, those guilty of transmitting bomb hoaxes can be fined up to \$50,000 or jailed up to seven years, or both (Soh and Dawson, 2002).

Noting trends in the USA and the European Union, the International Chamber of Commerce (ICC) has strongly criticized the attempts of governments all over the world to compel communication service providers to store end-user traffic data. According to the ICC this practice is neither economically efficient nor effective for criminal investigation. The ICC expressed concerns about end-users privacy and recommended transparent and effective oversight procedures to prevent abuses and to protect user confidence. More importantly, it recognized that there has been insufficient public input and multi-lateral harmonization and felt that this could impair a competitive and dynamic communications and IT services market (ICC, 4. June 2003).

Governments however justify what they do, citing 'national security' or 'internal order', and corporations justify their actions in terms of 'lubricating market mechanisms'. Accordingly, Internet surveillance is thus promoted as 'necessary' in order to 'maintain strong states and to develop mature markets'. Accountability and the protection of privacy, however, is inadequate (Lyon, 2003).

Conclusion: Dumbing Down Democracy

Broadly, the period from 1998 to 2000 was the time when much online political activity emerged and grew. It has taken some countries longer to introduce specific cyber-legislation and impose restrictions. It was not until 2000 that the Indian government passed the Information Technology Act. Authorities in countries such as Cambodia have so far made no efforts to regulate or restrict the Internet, and Malaysia stands by its promise not to censor Internet content. The lack of restrictions in these countries stems from either indifference due to a low level of Internet penetration and access making the medium irrelevant as a tool of political dissent, or, as in the case of Malaysia, a desire not to deter foreign investment.

But by the year 2000 there were signs that efforts to contain political cyber activism were about to emerge and this became the dominant trend when the after-effects of 911 swept into the region. Political expressions that blossomed with the arrival of the Internet on many occasions and in many ways are being brought under legislative control. As a result, the Internet has itself become a target for censorship, regulation and control.

However, the absence of specific regulations governing the Internet has not prevented many governments from using other legislation and intimidation to control Internet content and cyber-dissidents. In many Asian countries the new possibilities for free expression that accompanied the advent of the Internet still carry the old risks of persecution (Menon, 2001). The repressive practices of media control, from the colonial era to post-colonial and contemporary governments, have now been adapted and applied to the Internet and information carried by mobile information devices.

Hence, we can question the argument that the media has indeed a key position in the development of democracy. If we take the Internet as an extension of the mass media in that it offers one-to-many communication via websites and email lists, the hope of democratic potential that was placed on new media seems to be misplaced after all, given the increased legislations against it. New media is not as free as it was originally deemed to be.

Democracy requires a public culture of participation, but the stringency of post September 11 Internet-related legislations seem to lead to the opposite situation. People are reluctant to conduct political communication online given that state agencies, with the cooperation of commercial service providers, can be monitor, track and store them. Hence, people prefer to keep important information confidential and exchange in a low-tech or no tech manner. This is especially so in authoritarian regimes such as Burma, Vietnam and Singapore. In fact many surveys show that the percentage of websites and news groups oriented towards politics is rather small.

It is often said that that key institutions central to democracy such as political parties have become irrelevant in late modernity, or that official politics does not command the level of support and/or participation that it has in the past. It is also said that politics itself is fragmenting, and the focus is outside of the formal political process and institutions such as social movements, civil society and NGOs. If the Internet does not live up to the process of “new politics”, it seems to suggest that perhaps old-style politics may still be relevant and have a role to play in promoting democracy.

This is where traditional activism still plays a part and where the “traditional” methods are still relevant to get around the high-tech surveillance state. At the same time, new media technologies can still be relevant if they are used by human beings with ingenuity and determination. This underlines the importance of the “people” and their willingness to act.

Nevertheless, it remains to be seen if further innovations in information technology would allow cyber activists to by-pass the increasing tighter legal control. In the meantime it only serves to confirm that the democratic potential of the Internet is being dumbed down.

About the author

James Gomez is a writer and an activist. He founded the Think Centre (Singapore) <www.thinkcentre.org> on 16 July 1999 and published *Self-Censorship: Singapore's Shame* in September that year. James also co-founded Think Centre (Asia) <www.thinkcentreasia.org> in Bangkok in August 2001. He is presently Regional Research and Communications Manager, Friedrich Naumann Foundation, Regional Office, Thailand. Email: jamesgomez@hotmail.com

References

Amnesty International (2002) "Internet Restrictions: stifling freedom of expression from China to Tunisia", http://www.web.amnesty.org/mavp/av.nsf/pages/internet#south_korea

APEC media release (2003) "Conference on the Strengthening International Law Enforcement Cooperation to Prosecute Cyber Criminals, Hackers, and Virus Authors", Bangkok, 25 July.
http://www.apecsec.org.sg/apec/news___media/media_releases/250703_tha_strengthening_law.html

APEC media release (2003) "APEC Cybersecurity Tool Kit to be Developed for Corporations and SMEs", Chinese Taipei, 8 October.
http://www.apecsec.org.sg/apec/news___media/media_releases/081003_ct_cybersecurity.html

ASEAN: Work Programme to Implement the ASEAN Plan of Action to Combat Transnational Crime, Kuala Lumpur, 17 May 2002,
<http://202.154.12.3/5616.htm>

Asia Media Information & Communication Centre (2000) *Media and Democracy in Asia*, Singapore: AMIC.

The Australian (18 September 2002) "Court bans racist website",
<http://australianit.news.com.au/common/print/0,7208,5119879%5E16123%5E%5Enbv%5E,00.html>

Ayers, Michael C and McCaughey, Martha (2003) "Introduction", in Martha McCaughey (ed.) *Cyberactivism: Online Activism in Theory and Practice*, New York & London: Routledge.

Badam, Ramola Talwar (2004) "Police in India to monitor cybercafes", Boston.com, 18 January,
http://www.boston.com/business/technology/articles/2004/01/18/police_in_india_to_monitor_cybercafes/

ASIA RIGHTS Issue One: July 2004

Banerjee, Indrajit (2003) "Internet and democracy in Asia: a critical exploratory journey", in Indrajit Banerjee (ed.) *Rhetoric and Reality: The Internet Challenge for Democracy in Asia*, Singapore: Times Media Private Limited.

BBC News (23 July 2000) "India tackles cyber crime",
http://news.bbc.co.uk/1/hi/world/south_asia/847727.stm

Boas, Taylor C and Kalathel, Shanti (2003) *Open Networks, Closed Regimes: The Impact of the Internet on Authoritarian Rule*, Washington DC: Carnegie Endowment for International Peace.

China Post (19 February 2003) "Offices of Sportingbet's Taiwan promoter raided".
<http://www.chinapost.com.tw/taiwan/detail.asp?ID=35102&GRP=B>

China Study Group (2003) "China arrests factory worker who posted political essays online", 20 December.
<http://www.chinastudygroup.org/index.php?type=news&id=4064>

Chua, Hian Hou (2003) "Anti-spam laws in the making?", Computer Times online, 29 October, <http://computertimes.asia1.com.sg/news/story/0,5104,1497,00.html>

Committee to Protect Journalists (2002) "China: college student missing after posting essays online", <http://www.cpj.org/news/2002/China10dec02na.html>

Computer Crime Research Center (11 July 2003) "FBI training FIA officers on cyber crime", <http://www.crime-research.org/eng/news/2003/07/Mess1101.html>

Dahlgren, P (2001) "The transformation of democracy?" in Bernie Axford and Richard Huggins (eds) *New Media and Politics*, London: Sage

Elegant, Simon (2003) "Calm in the storm", TimeAsia, 5 May.

Elegant, Simon (2002) "Where will they strike next?", Time, 2 December.

Free Vietnam Alliance (2002) "Vietnam: new threats to free expression", 9 October.
<http://www.fva.org/200210/story03.htm>

Gambling Licenses Online (15 November 2002). China.
<http://www.gamblinglicenses.com/>

Go, Robert (2004) "Asia-Pac gets new centre to fight terror", The Straits Times, 5 February.

ASIA RIGHTS Issue One: July 2004

Go, Robert (2004) “25 nations unite on cross-border terror”, *The Straits Times*, 6 February.

Gomez, J and Smith, A (2003) “Introduction”, in Uwe Johannsen, Alan Smith and James Gomez (eds.) *September 11 and Political Freedom: Asian Perspectives*, Singapore: Select Publishing.

Ho, K.C., Kluver, Randolph and Yang, Kenneth C.C. (2003) “Asia encounters the Internet”, in K.C. Ho, Randolph Kluver and Kenneth C.C. Yang (eds) *Asia.com: Asia Encounters the Internet*, London and New York: RoutledgeCurzon.

IFEX (2003) “Cyber-dissident Nguyen Khac Toan sentenced to 12 years in prison”, 3 January. <http://www.ifex.org/fr/layout/set/print/content/view/full/18217/>

IFEX (2003) “Cyber-dissident Kong Youping arrested; court rejects appeal hearing for dissident He Depu”, 23 December. <http://www.ifex.org/en/layout/set/print/content/view/full/55812/>

Ignotus, Miles (2004) “Censoring the Web”, *Bangkok Post*, 15 February.

Index On Censorship (2002) “Pakistan: keeping tabs on web users”, 6 August. http://www.indexonline.org/indexindex/20020806_pakistan.shtml

Index On Censorship (2004) “Vietnam: online dissident journalist jailed”, 6 January. http://www.indexonline.org/indexindex/20040601_vietnam.shtml

India Information Technology Act (2000). http://www.mit.gov.in/itbillonline/it_framef.asp

International Chamber of Commerce (4 June 2003) “Common Industry Statement on Storage of Traffic Data for Law Enforcement Purposes”, http://www.iccwbo.org/home/statements_rules/statements/2003/Common%20Industry%20Position%20on%20data%20retention%20final%20june%202003%20logos.pdf

The Korea Times (10 March 2003) “Law revision bans gambling at PC rooms, Internet cafes”, <http://times.hankooki.com/lpage/nation/200303/kt2003031017174011980.htm>

Kyu Ho Youm (2003) “The Internet and Democracy in Asia”, in Indrajit Banerjee (ed.) *Rhetoric and Reality: The Internet and Challenge for Democracy in Asia*, Singapore: Eastern Universities Press.

Lintner, Bertil (2001) “Denial of access”, in Sheila Coronel (ed.) *The Right to Know: Access to Information in Southeast Asia*, Philippines Center for Investigative Journalism, pp. 21-41.

Luwarso, Lukas (2004) "Manufacturing control: new legislations threatens democratic gains in Indonesia", in Steven Gan, James Gomez and Uwe Johannen (eds) *Asian Cyberactivism: Freedom of Expression and Media Censorship*, Bangkok: Friedrich Naumann Foundation.

Lyon, David (2003) "Cyberspace, surveillance, and social control", in Ho, K.C., Kluver, Randolph, Yang, Kenneth C.C., eds., *Asia.com: Asia encounters the Internet*, London: RoutledgeCurzon.

Menon, Kavita (2001) Asia 2001 Overview, Committee to Protect Journalists (CPJ). <http://www.cpj.org/attacks01/asia01/asia.html>

Menon, Vijay (1999) Informatik Forum 1/99: Internet in Asia. <http://www.interasia.org/results/if9901preface.html>

Neumann, A. Lin (2001) "The great firewall", Committee to Protect Journalists. http://www.cpj.org/Briefings/2001/China_jan01/China_jan01.html

Newindpress.com (4 February 2004)
"CBI tie up with Asian countries to fight cyber crime", <http://www.newindpress.com/Print.asp?ID=IEH20030206124234>,
<http://www.newindpress.com/Newsitems.asp?ID=IEH20030206124234&Title=Top+Stories&rLink=0>

The New Paper (2002) "Your SMS is private, telcos say", 19 December.

The New Paper (2004) "Service provider: SMS confidential but...", 2 February.

Pabico, Alecks P. (2003) "New media as big brother: the Philippines after September 11" in Steven Gan, James Gomez and Uwe Johannen (eds.) *Asian Cyberactivism: Freedom of Expression and Media Censorship*, Bangkok: Friedrich Naumann Foundation.

PRC Interim Regulations Governing the Management of International Computer Networks (1996). People's Republic of China, State Council Order No. 195, Article 13.

Privacy International and the Electronic Privacy Information Center (2002) Privacy & Human Rights 2002: An International Survey of Privacy Laws and Developments. <http://www.privacyinternational.org/survey/phr2002/>

Privacy International (2003) Privacy and Human Rights 2003: Executive Summary. <http://www.privacyinternational.org/survey/phr2003/executivesummary.htm>

Reporters Sans Frontieres (2002) Vietnam annual report 2002. http://www.rsfs.org/article.php3?id_article=1429

Reporters Sans Frontieres (2002) 11 September 2001 – 11 September 2002: The Internet on Probation: Anti-terrorism drive threatens Internet freedoms worldwide, 5 September. http://www.rsf.fr/article.php3?id_article=3671

Reporters Sans Frontieres (2002) Torture, Arbitrary Detention and Self-Censorship. Four Months Later: Consequences of the State of Emergency and of the Fight Against “Maoist Terrorism” Attacks on Freedom of the Press, 26 March. http://www.rsf.fr/article.php3?id_article=902

Reporters Sans Frontieres (2003) Pakistan press release, 18 June. http://www.rsf.org/print.php3?id_article=7245

Reporters Sans Frontieres (2004) Press Freedom Barometer. http://www.rsf.fr/rubrique.php3?id_rubrique=119

Reporters Sans Frontieres (2004) “2003, a black year”, 6 January. http://www.rsf.org/article.php3?id_article=8969

Reporters Sans Frontieres (2003) Thailand press release, 18 June. http://www.rsf.org/print.php3?id_article=7251

Reporters Sans Frontieres (2004) “Vietnam press release, 18 June. http://www.rsf.org/print.php3?id_article=7252

Rozumilowicz, Beata (2000) “Democratic change: a theoretical perspective”, in Gunther, Richard and Mughan, Anthony (eds.) *Democracy and the Media: a comparative perspective*, London and New York: Routledge.

Singapore Internet Code of Conduct (1997). http://www.sba.gov.sg/sba/i_codenpractice.jsp

Soh, N and Dawson, S (2002) “Fear for safety fuelled SMS bomb hoax”, The Straits Times, 30 November.

SunStar Network Online (2002) “PNP goes on alert, traces ‘prankster’”, 20 October.

Tharoor, Shashi (2003) “The ‘cyber summit’: a chance to expand the information society”, International Herald Tribune, 17 October.

Tkach-Kawasaki, Leslie M. (2003) “Clicking for votes: assessing Japanese political campaigns on the web”, in K.C. Ho, Randolph Kluver and Kenneth C.C. Yang (eds) *Asia.com: Asia Encounters the Internet*, London and New York: RoutledgeCurzon.

USA TODAY (19 September 2003) “South East Asia unveils cyber crime fighting plan”, www.usatoday.com/tech/world/2003-09-19-asean-on-cybercrime_x.htm

Ward, M (2004) “Snooping industry set to grow”, BBC News World Edition, 21 January. <http://news.bbc.co.uk/2/hi/technology/3414531.stm>

Williams, M (2000) “Japan's police gain right to tap phones and e-mail”, CNN.com, 16 August. <http://www.cnn.com/2000/TECH/computing/08/16/japan.police.idg/>

Wong, J (2001) “Singapore limits election politics on Internet”, Reuters, 13 August. <http://www.singapore-window.org/sw01/010813re.htm>

WSIS Declaration of Principles (2003) “Building the Information Society: a global challenge in the new Millennium”, Geneva, 12 December. http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!MSW-E.doc

Young, D and Kane, Y. I. (2004) “How spammers are targeting mobile phones in Asia”, Reuters, 3 February. <http://sg.news.yahoo.com/040203/3/3hpt1.html>

Zaw Oo (2004) “Mobilising Online: the Burmese cyber strategy against the Junta”, in Steven Gan, James Gomez and Uwe Johannsen (eds) *Asian Cyberactivism: Freedom of Expression and Media Censorship*, Bangkok: Friedrich Naumann Foundation.
