

11 September 2001 – 11 September 2002

The Internet on probation

Reporters Without Borders defends freedom of expression. This goes hand in hand with press freedom but also with the free flow of information on the Internet and preservation of confidentiality there. This report highlights the serious battering the Internet has suffered since the 11 September attacks in the United States.

Since the mid-1990s, a number of governments and international institutions have sought to control the Internet through laws and regulations. They have been quite successful. The campaign against terrorism and the security excesses it produces have speeded up the trend.

One year after the tragic events in New York and Washington, the Internet can be added to the list of “collateral damage” caused by the general spate of security measures. As a result, basic cyber-freedoms have been cut back.

The countries usually criticised for not respecting human rights and freedom of expression – such as China, Vietnam, Saudi Arabia and Tunisia – have become schizophrenic about the Internet. They have encouraged its growth as a tool of state propaganda or economic interests, but at the same time moved to control it and clamp down on criticism, argument and hopes for democracy expressed online.

Since the 11 September attacks, these “enemies” of the Internet have taken advantage of the international drive against terrorism to strengthen the police and legal machinery they have installed to put the Internet under surveillance. They are also using it to step up pressure on cyber-dissidents.

This is what has happened in China where the government is trying to contain the growth of cybercafés and where, on 30 August this year, there were 30 Internet users imprisoned. Some 14,000 cybercafes were closed in the space of a few weeks this summer. A cyber-dissident was sentenced in August this year to a record 11 years in prison. The authorities have also obliged Internet service providers (ISPs) and Web portals to sign self-censorship agreements. In a major error, the US giant Yahoo! was among those who signed.

In Tunisia, the regime of President Zine el-Abidine Ben Ali is also skilfully riding the wave of anti-terrorist measures to tighten the screws on cyber-dissidents. This June, one of his strong critics, Zouhair Yahyaoui, founder of the website *Tunezine.com*, was sent to prison for two years and four months.

But the Internet is not just under siege in countries traditionally hostile to freedom of expression. It is also threatened in Western democracies, where many countries have passed

laws, taken measures and adopted practices that are putting the Internet under the ferrule of the security services. These governments are introducing generalised retention of details of e-mails sent and received and of what websites people visit.. This turns ISPs and telephone companies into a potential arm of the police. Access to this mass of information is being given with alarming ease to police and intelligence services. This unprecedented abuse means all citizens are theoretically under suspicion.

Such measures include Resolution 1373 on fighting terrorism, approved by the United Nations Security Council on 28 September last year; the USA Patriot Act adopted by the US Congress on 24 October last year and various orders of President George Bush before and after this act; the amendment of the European Directive on Protection of Telecommunications Data and Information approved by the European Parliament on 30 May this year; the passing of laws by the parliaments of many countries around the world; and the recommendations of the G8 nations summit and of the European police body, Europol.

The United States, Britain, France, Germany, Spain, Italy, Denmark, the European Parliament, the Council of Europe and the G8 nations have all challenged cyber-freedoms over the past year. Yet these are countries with secular and democratic traditions whose citizens fought long and hard to win their right to free expression, the confidentiality of mail and the right of journalists not to reveal their sources.

What would the citizens of Europe and elsewhere do if they were told a law had been passed allowing what they sent through the post to be routinely read by the police at any time? They would be outraged at such restrictions on their freedom. Yet these are exactly the kind of measures that have been taken or are being taken concerning the Internet. We therefore need to be much more vigilant.

Germany

The “Otto-Katalog” (a reference to a general mail-order catalogue): this is the nickname the media and NGOs have given the package of anti-terrorist measures devised by interior minister Otto Schily and adopted by parliament at the end of last year. The content of the law was sharply attacked by organisations defending civil liberties, freedom of expression and the privacy of personal data. The most controversial measures related to abolition of the distinction between the police and the intelligence services, who now have unlimited access to the police database INPOL.

They also have access to computer-held telecommunications records, including the content of messages, data about e-mail exchanges, data allowing the authors of such messages to be found and access to phone company records.

About 20 organisations have formed a coalition to denounce Schily’s efforts to monitor such traffic as “a law whose legal basis is dubious, unclear and hard to assess, a law that will also not stop terrorist activity.”

Privacy International even awarded Schily its annual Big Brother Award for what it called his policy of spying and curbing collective and individual freedoms. It said he had contributed, under cover of the fight against terrorism, to reducing the rights of German citizens, especially the right to keep details of their personal life confidential.

Canada

Close surveillance of the Internet and e-mail is the core of Canada's C-36 anti-terrorist law, passed in mid-December last year, which makes it easier for the police to get permission to install telephone and computer listening devices. The Communications Security Establishment, a department of the defence ministry, can also for the first time in its history, listen in to both Canadian and foreign citizens. The confidentiality of e-mail correspondence has clearly been destroyed.

Information commissioner John Reid, an independent official who monitors respect for civil liberties in Canada, protested indignantly in a letter to the chairman of the federal senate's justice committee, Joyce Fairburn, that the new law struck "a crippling blow" at his independence and his ability to protect a citizen's right to confidentiality.

Denmark

In October last year, the Danish government proposed major amendments to key national laws so as to combat terrorism more effectively. Under this blanket heading, they affected laws concerning justice, internal affairs, the economy and taxation.

The Internet and new technology have been especially targeted. The government asked the justice ministry to take steps to legalise retention of details of phone calls, Internet activity and e-mails and to allow police faster and easier access to such material. On 31 May this year, the law authorised officials to keep data of this kind for up to a year. The anti-terrorist law went further, by allowing the intelligence services (PET) and the police to freely consult this data without prior permission by a judge. The police can even install on the equipment of ISPs e-mail interception technology similar to the Carnivore programme used in the United States.

Spain

The lower house of the Spanish parliament passed an Internet law, the LSSICE, on 27 June this year, with the aim of fighting cyber-crime and terrorism on the Internet in Spain. The measure, put together by the science and technology ministry, includes anti-freedom clauses in the eyes of those who believe that the Internet should exist with minimal controls. The law obliges ISPs to keep details of their customers' Internet and e-mail activity for at least a year. But opposition deputies managed to push through an amendment to bar police and intelligence officials from using such data without court permission.

Opponents of the new law were dismayed because they expected the deputies to water down the original bill. In fact, the final version was more repressive than the initial draft, especially where ISP retention of connection records is concerned. The methods to store such data are not spelled out, which has raised fear of abuses. It remains to be seen which authorities will be able to shut down sites deemed to have "harmed values" without undermining freedom of expression. This freedom is recognised and defended in the national Constitution, whose Article 20 notably protects the right to "freely send or receive truthful information by any means of communication."

United States

The 11 September attacks in New York and Washington last year and 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.

The campaign to get control of the Internet began just a few hours after the attacks, when FBI agents went to the head offices of the country's main ISPs, including Hotmail, AOL and Earthlink, to confiscate details of possible e-mail messages between the terrorists. The online magazine *Wired* reported that FBI agents also tried to install the Carnivore surveillance system (since renamed DCS 1000) on the main ISPs based in the United States.

It said they had turned up at ISP offices with the software and offered to pay the cost of installation and circuits. They had demanded and obtained material from certain e-mail accounts, most of whose names began with the word "Allah."

Carnivore: a programme with a wide sweep

Carnivore, devised by FBI experts, is the first major electronic surveillance software to be used by a national police force. When installed on an ISP, it can record and store all the messages sent or received traffic by the ISP's customers. Civil liberties advocates in the United States fought against it and it had hitherto never been used without prior permission of a judge. A law known as the Combating Terrorism Act, passed urgently by the Senate on 13 September, two days after the attacks, allowed the intelligence services to use it without having to seek such approval.

Many US officials began criticising encryption, which allows Internet users to keep their Internet messages and activity confidential by encoding it with software. Again on 13 September, Republican Sen. Judd Gregg, in a speech before the US Congress, called for the banning of all encryption software whose makers did not supply the decoding key to the authorities. This was needed, he said, because the FBI had taken 10 months to decode encrypted files in the computer of the person mainly responsible for the first attack on the World Trade Center in 1993.

David Zimmerman, inventor of the current leading encryption programme, PGP, pointed out that society had more to gain than to lose from powerful encryption, which could save lives around the world. PGP was used by human rights organisations everywhere, especially in countries ruled by dictatorships, he said.

Easing of electronic surveillance regulations

Monitoring of data on the Internet was legalised on 24 October last year when the US House of Representatives passed the "USA Patriot Act," later renamed the "USA Act." This anti-terrorist measure confirmed the authority already given to the FBI to install the Carnivore programme on an ISP's equipment to monitor the flow of e-mail messages and store records of Web activity by people suspected of having contact with a foreign power. This requires only the permission of a special court.

The abuses feared by freedom of expression campaigners materialised. This spring, a US group, the Electronic Privacy Information Center (EPIC), after a legal battle with the FBI, won the right to see some material relating to the Carnivore programme. EPIC's experts found that, as part of the anti-terrorist drive, the e-mail traffic of innocent private citizens had been intercepted and spied on, in what the FBI said was "an error" caused by technical foul-ups.

Encryption software has come under attack from the FBI's Magic Lantern programme, a virus sent by e-mail that can secretly record the keystrokes of an Internet user. This enables

the FBI to see the code employed by encryption users and so recuperate messages written by the computer owner.

As well as trying to monitor the flow of information on the Internet to check what is being said and exchanged, the authorities are also trying to use the Internet to put out US propaganda in their war against terrorism.

The *New York Times* reported on 19 February this year that the Defense Department's Office of Strategic Influence (OSI) had proposed planting disinformation in the foreign media, mainly through websites set up and secretly run by the OSI and through e-mails sent to journalists or their offices. The revelation caused an outcry and White House spokesman Ari Fleischer quickly said President Bush knew nothing about the project and had ordered the OSI closed down.

The world's Internet cop

The US justice department also reserved the right to prosecute Internet "hackers," whether or not they were Americans or living on US territory. The authorities argued that since most Internet traffic passed through the United States, they would pursue anyone, anywhere in the world, who broke US laws concerning cyberspace as soon as the target of such electronic "crimes" passed through US channels.

This step, a worldwide first, gave the United States the unofficial role of the planet's "Internet cop," civil liberties campaigners protested. But hacking can cover many activities. According to Internet security expert Mark Rasch, those responsible for any routine Internet offence – stealing computer data, minor hacking into websites or sending pornographic pictures – could be targeted by the US authorities.

A rare event in the history of the Internet in November last year showed the degree of US determination. Somalia was completely cut off from the Net after the country's only ISP, the Somalia Internet Company, and the main telecommunications firm, Barakat, were forced to shut down after being accused by the US of funding Osama bin Laden's Al-Qaeda network and being put on the US list of those supporting terrorism. For two months, Somalis had no Internet access. It was restored in January this year, when a new ISP, NetXchange, began operating.

US attorney-general John Ashcroft and FBI director Robert Mueller presented a plan to reform the FBI on 30 May this year that would refocus its activities towards anti-terrorism at the expense of fighting crime. One major change was that FBI agents would have a free hand, without needing court approval, to install listening devices on the phones and computers of anyone suspected of having information about terrorist activity. The FBI would also be able to delve into databases to get commercial, economic or scientific information. Such searches could be carried out for precautionary reasons, even if there was no evidence against the people or organisations being monitored.

France

The drive for security set off by the 11 September attacks saw the passing of two laws in France to restrict cyber-freedoms. The government of prime minister Lionel Jospin presented a package of anti-terrorism measures in November last year called the Law on Everyday Security (LSQ). This was not specially designed to fight terrorism: clauses were hastily added to an existing measure, the Law on the Information Society (LSI).

The LSQ, urgently and almost unanimously approved on 15 November without any discussion, extended to a year the period that records of Internet activity and e-mail traffic

were to be kept by ISPs. It also permitted judges to use “secret state measures justified as being for national defence purposes” to decode e-mail messages and required encryption firms to hand over their codes so the authorities could read the messages. These measures put the Internet in France under tight surveillance and severely hampered encryption.

Campaigners for freedom of expression on the Internet (such as LSIjolie, IRIS, Bug Brother, Reporters Without Borders) protested against such hasty passage of a measure that had not been discussed or negotiated and which threatened the principle of confidentiality in professional and private communications, especially the right of journalists not to reveal their sources.

Searches and confiscation of online data

The new government of prime minister Jean-Pierre Raffarin presented another measure to parliament this July, the “Internal Security Guidance and Planning Law” (LOPSI), which contained clauses that aroused concern about online freedom of expression and individual rights to confidentiality.

LOPSI, which was passed on 31 July, raised very delicate issues, mainly its provision for a further measure to give police the power to make remote online searches of ISPs and their records of customers’ Internet activities and private and professional e-mail traffic. This would allow police, with a judge’s permission, to have “direct access to data deemed necessary to establish the truth.”

LOPSI’s critics, such as the judges’ trade union, IRIS and the Computer Freedom Federation (FIL), wonder whether this further measure, detailing how the law is to be applied, will be properly debated in parliament. Will the police detectives authorised to access and seize the computer files be specially trained and equipped for the job? Will they be obliged, as in normal search operations, to inform the targeted computer users what is being done? Will the judges giving such authorisations be specially trained and made aware of their intrusive nature of such operations?

It also says the measure will allow the use, under legal supervision, of “the most advanced techniques” to intercept messages and the establishment of sophisticated surveillance because of the “increasingly routine use by criminals of methods to conceal their communications and encounters.” The measure directly affects those who use encryption to preserve their anonymity online.

United Kingdom

The Anti-Terrorism, Crime and Security Act passed in Britain in mid-December last year extended to at least a year the period ISPs are obliged to keep details of people’s Internet activity. The home secretary (interior minister) also said he would have the power to monitor online financial transactions and private e-mail traffic. The new law exempts police in many cases from having to get prior permission from a judge. They would only need a go-ahead from the home secretary or one of his top aides. The measures caused uproar and some ISPs said they were thinking of moving their operations to another country.

NGO fears of major security excesses seem well-founded. In mid-June this year, home secretary David Blunkett, proposed amendments to a controversial law passed in 2000, the Regulation of Investigatory Powers Act (RIPA), to give local authorities (such as tax offices, social security and municipal services) access to data on citizens’ Internet activity and to their e-mail. The proposal aroused such opposition from the media and civil liberty groups that the government decided to postpone the measure until the autumn.

“Unconstitutional” laws?

Elizabeth France, Britain’s information commissioner, an independent figure monitoring respect for citizens’ rights to keep personal data confidential, threw a spanner in the works in early August this year by saying that the two measures conflicted and were improper.

Her office said the anti-terrorist law stipulated that Internet activity data could only be retained longer than was needed by ISPs for their accounting purposes if it was needed for enquiries related to national security. Yet the RIPA allowed access to it, with no real legal permission, in cases that mostly had no national security link. This, her office said, meant there was every chance that access granted to such data would be declared illegal under personal privacy and human rights legislation.

India

The POTO (Prevention of Terrorism Ordinance) anti-terrorist law passed in the wake of the 11 September attacks allowed the government to monitor all types of communications, especially electronic exchanges such as e-mail, all without prior legal or official permission. The information gathered from such interception ordered by the security services can be used as evidence in court against a person.

Journalists, as important Internet and e-mail users in India, were especially threatened under the law, which initially said reporters who refused to hand over to the authorities evidence they had concerning terrorists or organisations classified as such could be sent to prison for five years.

The law was amended after strong criticism by the opposition and human rights and freedom of expression campaigners and the clause obliging journalists to reveal information linked to cases of terrorism was removed.

Italy

The government pushed through an anti-terrorism measure in mid-December last year that considerably eased setting up surveillance of suspect individuals and also gave a green light to intercept e-mail and retain records of Internet and other telecommunications activity.

The new law greatly increased the number of police and security officials authorised to take such steps and more lower grade officials were given such powers. On top of this, those who reveal the names of such officials and details of how such surveillance is initiated and carried out face prison sentences. NGOs are therefore worried about the many civil servants who will now have access to details of people’s Internet activity.

At the end of last year, another law was passed that aimed to reform the intelligence services, giving agents of the civil branch (SISDE) and the military one (SISMI) complete freedom to commit crimes, except killing or injuring people, in the course of their work. These included theft, secret searches and illegal phone and Internet surveillance. Even though the secrecy of the intelligence services hides the nature of current surveillance, personal privacy and confidentiality campaigners attacked the measure as “opening the door to all kinds of excesses and to serious and mindless abuses in a major democratic country.”

Italy, which held the presidency of the G8 group of countries at the time of the 11 September attacks, also laid the first stone, in a government statement eight days after the

attacks, of a policy of “fighting Internet and high tech crimes.” This policy has involved increasing the powers, resources and activities of the informal G8 network.

Italy takes the lead among the G8 group

Officials at the meeting in Canada in June this year of eight G8 heads of government noted that the network of originally 16 (now 26) countries enabled speedy cooperation between international police organisations when urgent response was required in high tech crimes, including Internet messages between terrorists and other criminals.

Without further explanation, the G8 summit said legal experts and police authorities had developed ways of determining the origin, destination and route of terrorist or criminal traffic on the Internet; of more easily gathering electronic evidence for this; and of ensuring retention of existing electronic evidence so it could not be deleted or changed.

Cyber-freedom organisations, especially some members of the Global Internet Liberty Campaign (GILC), note that Italy is one of the countries that has most insistently pressed the European Parliament to amend its Directive on Protection of Telecommunications Data and Information (see section on the European Union). The amendment, approved on 30 May this year, requires the storing of phone and Internet connection records (traffic logs). The NGOs point out that the list of logs to be stored as a result of the amendment is almost identical to the recommendations of the G8 experts. Many see the hand of Italy behind such major international measures.

European Union

The European Union was once strongly opposed to any kind of extensive and general electronic surveillance or investigation. But it sharply changed its tune after the 11 September attacks. The Council of the European Union fought energetically to impose the views of the 15 member-state governments on the European Parliament and to push through laws to impose, under US pressure, general retention of phone and Internet activity data.

Bush exerts his influence

In mid-October last year, President George Bush urged Belgian prime minister Guy Verhofstadt, the then-president of the European Union, to alter a proposed amendment to the Directive on Protection of Telecommunications Data and Information to take account of the fight against terrorism. The draft amendment provided for “preventive retention” of data on Internet activity (traffic logs). Bush expressed support for the position of the British government (which, like the French, has introduced such data retention) and of various European Union police officials calling for new powers to monitor more effectively phone and Internet activity.

Bush told Verhofstadt the United States opposed automatic deletion of Internet connection records, a principle upheld in the amendment being considered by the European Parliament. Concerned NGOs, such as Statewatch, denounced this as US interference in European affairs solely aimed at backing proposals made, but little supported, they said, by the EU’s “Council of 15” (Enfopol) police working party, which had been working for nearly two years to remove the principle of automatic deletion from the directive.

The position of Enfopol, like that of the US president, goes against that of the European Parliament’s Citizens’ Freedoms and Rights Committee, which in July last year

approved a first report by Italian Radical MEP Marco Cappato for strict supervision of police access to traffic logs retained by phone companies and ISPs.

Against the opinion of legal experts and the Freedoms and Rights Committee

The Cappato report also said that if such practices were to be allowed, EU member-states should be obliged to act under “a specific law comprehensible to the general public.” The measures would have to be “entirely exceptional, authorised by the judicial or competent authorities for individual cases and for a limited duration, appropriate, proportionate and necessary within a democratic society.” They should also be in line with EU human rights rulings, which forbid all forms of “wide-scale general or exploratory electronic surveillance.”

The position of the European Parliament changed markedly in less than a year. Under intense pressure from the Council of the European Union (that groups all member-states), Euro MPs approved the amended directive on 30 May this year, against the advice of Cappato, who presented the original proposed amendment.

Article 15.1 of the new directive obliges governments that do not yet have such legislation, to pass laws (within 15 months) to force ISPs and phone companies to retain all records of e-mails, Internet activity, faxes and phone calls that have passed through their hands and guarantee the police, the courts and some government bodies free access to it.

A report by the Council of 15’s legal department released on 15 October last year, had said however that EU governments already had the necessary powers to intercept telecommunications to fight terrorism, implying that the newly-amended European-level directive was superfluous.

Governments approve Convention on Cybercrime

The first International Convention on Cybercrime was signed by 30 countries in Budapest in November last year. The pact, which was prepared over four years, initially concerns European countries. In the wake of the 11 September attacks, it was signed by (among others) the United States, Canada, Japan and South Africa. Twenty-six of the Council of Europe’s 43 members signed. “This agreement comes just at the right moment to fight against cyber-terrorism after the terrible attacks in the United States,” said Council of Europe deputy secretary-general Hans Christian Krueger. The agreement will enable centralisation of electronic evidence of offences linked to terrorism and organised crime on the Internet.

The agreement was attacked by civil liberties campaigners, ISPs and cyberspace experts who called it anti-freedom, meddling and encouraging a new era of generalised surveillance. Especially criticised were its articles 19, 20 and 21, which give details of the means of gathering private Internet data and activity records and data of interest to security services for their investigations; gathering records kept by ISPs; searching websites and their ISPs and the extension of such searches to other computer networks if necessary; storage of the data seized; and the real-time gathering of records and traffic logs if necessary (when legal officials ask ISPs to do this work themselves).

“General surveillance” of Europeans

The situation may get even worse. Euro MP Cappato disclosed that the Danish presidency of the EU proposed a measure on 24 June this year that the Council of the European Union might be in favour of. It was called “information technology related measures concerning the investigation and prosecution of organised crime” and said that “in the near future, all member-states will need to have adopted suitable measures to oblige telephone companies

and ISPs to retain all records of their traffic so security services can readily consult it in the course of their investigations.” Cappato says the Danish EU presidency is trying to move further towards “general surveillance” of European citizens.