Internet privacy threatened following terrorist attacks on US

Mike Ingram
24 September 2001

Governments around the world are using the terror attacks on the US to remove all privacy protection from Internet users.

Within two days of the September 11 bombings, the US Senate unanimously approved the "Combating Terrorism Act of 2001." Tagged on the end of the annual spending bill that funds the Commerce, Justice and State Departments, the Act greatly extends powers of surveillance, allowing prosecutors to authorise surveillance for 48-hour periods without the approval of a judge, under certain circumstances.

Proposed by Utah Republican Orrin Hatch and California Democrat Dianne Feinstein, the bipartisan measure stipulates that any US or state attorney general can order the installation of the FBI's controversial "Carnivore" email surveillance system. This nullifies previous restrictions on the use of Carnivore and other Internet surveillance techniques. Circumstances that do not require court orders include an "immediate threat to the national security interests of the United States, immediate threat to public health or safety or an attack on the integrity or availability of a protected computer."

Further legislation is expected, with repeated calls being made to ban encryption technology unless government agencies are provided with a means to decode messages.

Two of the USA's biggest Internet Service Providers (ISP), America Online (AOL) and Earthlink, are cooperating with security forces in their hunt for the perpetrators of the September 11 bombings. Dan Greenfield, spokesman for Earthlink, which has five million subscribers and more than 8,800 dial-up points around the US, was served with a subpoena on the day of the attacks and said the company is "fully cooperating with the FBI in light of the tragedy." He said it was "a very specific request. They are not installing monitoring equipment."

AOL has said it was not asked to install Carnivore, but is cooperating with the authorities following a subpoena. Spokesman Nicholas Graham said that AOL would not implement a system like Carnivore. "We don't allow access to our systems or our technology—we have a way to provide the information that law enforcement needs, and we do it ourselves," Graham said. Membership of AOL recently passed 31 million accounts, with more than seven million added during the past year alone.

The new Act gives the security services access to a massive amount of information on Internet users in the US and elsewhere. ISPs have been requested not to destroy log files which record the online activity of all users, including emails sent, web sites visited and even the terms entered into popular search engines such as Yahoo and Google. Some Internet Service Providers have the capacity to trace an email back to a specific user and can then obtain the user's account information, including their name, address, phone number and credit card details.

In response to the vast amount of information routinely held by ISPs, a number of web services have emerged that are designed to facilitate anonymous browsing and email. One such service, MagusNet, lets users visit Web sites by routing their requests through a series of Web servers. Users of MagusNet can visit a Web-based e-mail service such as Yahoo or Hotmail, and send messages that cannot be traced to the sender.

The originator of MagusNet, Jean Francois, closed the service immediately after Tuesday's attack in order to shield himself from possible interrogation. "The initial reaction I expect to see is a backlash against the anonymous service providers," he told the *Boston Globe*.

Even within the narrow confines of the US Senate, the scope of the new Act could not help but provoke alarm. During the floor debate Thursday, Senator Patrick Leahy (Democrat) and head of the Judiciary Committee, said that the legislation went far beyond merely thwarting terrorism and could endanger the privacy of Americans. Leahy pointed out that he only had the opportunity to read the Combating Terrorism Act just 30 minutes before the floor debate began. "Maybe the Senate wants to just go ahead and adopt new abilities to wiretap our citizens. Maybe they want to adopt new abilities to go into people's computers. Maybe that will make us feel safer. Maybe. And maybe what the terrorists have done is made us a little bit less safe. Maybe they have increased Big Brother in this country."

Republican Senator Jon Kyl, one of the Act's co-sponsors, said it would give former FBI Director Louis Freeh what he had lobbied for years ago: "These are the kinds of things that law enforcement has asked us for. This combination is relatively modest in comparison with the kind of terrorist attack we have just suffered."

There is no evidence that the measures now being proposed would have prevented the tragic events in New York and Washington. Rather, the legislation seeks to utilise an atmosphere of panic to take forward longstanding plans to subvert and even remove constitutional guarantees afforded to US citizens.

The Clinton administration had already made a number of attempts to outlaw or severely curtail encryption technology. The

most widely known and used public key encryption software, Pretty Good Privacy (PGP), was for years banned for export from the US. Its author Phillip Zimmerman became the subject of a protracted FBI investigation, as a result of his refusal to incorporate a backdoor in the software allowing the security services access to encrypted mail.

With the advent of Internet commerce, it became impossible for the US to oppose the use of encryption unilaterally, and subsequent efforts focused on demands for a global prohibition on encryption products without backdoors for government surveillance.

At the same time, the Clinton administration was developing the so-called "Clipper Chip"—a cryptographic device that included both a data-scrambling capability and a facility enabling government officials to decrypt any Clipper-encoded communications they intercepted. Following public outcry over the implications of this for civil liberties, the administration abandoned its plans to convince manufacturers to build Clipper-enabled products.

Far from being extraordinary measures dictated by the Bush administration's "war on terrorism", the latest legislation is the high point of a concerted attempt by the leading nations to curtail the role of the Internet as a platform for the free exchange of ideas. Prior to the terrorist attacks, the most frequently invoked rationale for the restriction of the Internet was its role in organising the anti-globalisation protests in Seattle and Genoa.

In May this year, the technology website *silicom.com* carried an article headlined "Privacy scandal: Dodgy data laws on the way." The article drew attention to documents obtained by the campaign group *Statewatch* relating to a joint offensive by the French, German and UK governments against Europe's data privacy laws.

"The documents reveal the Council of the European Union has given its backing to plans permitting the retention of phone, email, fax and internet communication data for up to seven years, giving law enforcement agencies the ability to 'fish' for criminal activity," the article says.

"The draft proposal claims the obligation on operators to erase and make traffic data anonymous 'seriously obstructs' criminal investigations. It calls on the European Commission to take 'immediate action' to ensure that law enforcement agencies can have access," *silicom.com* adds.

According to the article, the plans date back to 1995 when Europe adopted a trans-Atlantic interception agreement with the FBI. "A move in 1998 to extend the so-called Enfopol legislation to include the Internet failed, leaving individual countries to create their own interception laws, such as the UK's RIP Act."

The Regulation of Investigatory Powers (RIP) Act gives Britain some of the most advanced capabilities for Internet spying in the world. It requires ISPs to install a so-called "black box" device allowing access by the security forces to email messages hosted on the company's servers. The black box can also transfer data over secure channels to a new Government Technical Assistance Centre, built at a cost of billions of pounds.

The RIP Act also gives police the power to demand that those whose email is intercepted hand over any software keys and passwords necessary to read encrypted messages. Failure to do so can result in up to two years imprisonment. Telling a third party that such a request has been made carries a possible five-year sentence.

In the last week, British ISPs have been asked by the National Hi-Tech crime unit to keep customer communications data in case the FBI requires it. The request only refers to email logs sent and received since September 11 and does not include the actual content of emails, nor is the request legally binding. Should ISPs refuse, however, it is widely anticipated the powers of the RIP Act would be invoked. These powers can also be used to demand sight of the contents of any email.

The mass media is playing a crucial role in conditioning public opinion to accept the destruction of civil liberties. Combining calls for caution with declarations that extreme circumstances require extreme measures, they harangue privacy campaigners and the population as a whole into an accepting that some "sacrifice of freedom" is inevitable in times of war, and constitutional concerns should be put aside.

Unashamedly welcoming this, the right wing *Daily Telegraph* in Britain commented:

"There are other current movements of which to take note... One is the retreat of human rights lawyers from the forefront of public life. America in a war mood will have no truck with tender concern for constitutional safeguards of the liberty of its enemies. The other, which ordinary Americans will have to learn to bear, is the interference with their liberty of instant electronic access to friends and services."

Asserting that the terrorist attack was coordinated on the Internet, the paper continues, "If Washington is serious in its determination to eliminate terrorism, it will have to forbid Internet providers to allow the transmission of encrypted messages... and close down any provider that refuses to comply."

Revealing the utter hostility to the relative lack of restrictions on the use of the Internet that permeates a section of the ruling class, the paper states: "Uncompliant providers on foreign territory should expect their buildings to be destroyed by cruise missiles. Once the Internet is implicated in the killing of Americans, its high-rolling days may be reckoned to be over."