Big Brother Obama: US to spy on Internet messaging

Regulations to target Skype, Facebook, Blackberry

By Patrick Martin
28 September 2010

The Obama White House is backing new regulations that would compel popular Internet messaging services like Facebook, Skype and Blackberry to open up their systems to FBI surveillance, the *New York Times* reported Monday, citing federal law enforcement and national security officials.

The threat to democratic rights goes far beyond anything envisioned by the Bush administration. The goal is to make all forms of electronic communication that use the Internet subject to wiretapping and interception by federal police agencies.

In the past few years there has been a large-scale shift from conventional telephone communication to Internet-based messaging, which is both cheaper and more secure.

"Investigators have been concerned for years that changing communications technology could damage their ability to conduct surveillance," the *Times* reported. "In recent months, officials from the FBI, the Justice Department, the National Security Agency, the White House and other agencies have been meeting to develop a proposed solution."

This would include drafting new statutory language to bring providers like Research in Motion, the Canadian-based company that makes Blackberry devices, under legal controls similar to those established by the 1994 Communications Assistance to Law Enforcement Act.

That legislation required telecommunications companies to make their call-processing systems accessible to federal government spying, whether the calls pass through conventional phone lines or cell phone relay towers.

One of the biggest issues will be a government demand that communications service providers change the structure of their hardware and software, providing a "back door" for the use of intelligence agencies and ensuring that government agents can break any encryption applied to messages either by the service provider or the customer.

The *Times* article did not raise any alarm over the prospect of government snooping on the private communications of hundreds of millions of people, whether in the United States or in other countries. Nor did it quote any objection to the proposal from civil liberties groups, although the American Civil Liberties Union quickly issued a statement calling the plan "a huge privacy invasion" that was "one more step toward conducting easy dragnet collection of Americans' most private communications."

The only downside suggested by the *Times* account was the existence of technical problems that might prove expensive and cumbersome for the corporations that would have to comply with the new rules, and that the new security procedures might create new opportunities for hackers.

FBI General Counsel Valerie Caproni, who discussed the issue with the newspaper, said that there was a consensus among police and intelligence agencies that companies which provide encrypted communications would have to retain the key to any encryption, rather than allowing their customers to devise and hold their own.

"No one should be promising their customers that they will thumb their nose at a US court order," she told the *Times*. "They can promise strong encryption. They just need to figure out how they can provide us plain text." In other words, encryption would protect the privacy of communications, except when the government says otherwise.

This is the same stance taken by dictatorial governments from China to the Middle East. The governments of Saudi Arabia and the United Arab Emirates only last month threatened to bar Blackberry services in their countries because Research in Motion refused to allow the local intelligence services to monitor and intercept messaging.

The *Times* article gave two examples of government efforts to intercept encrypted or peer-to-peer communications that ran into technical obstacles, one involving a drug cartel, the other related to the failed Times Square bombing earlier this year. These examples were chosen to support the claim by the Obama administration that the buildup of surveillance is part of a struggle against crime and "terrorism."

However, the Obama administration has defined "terrorism" so widely that the term now covers a vast array of constitutionally protected forms of political opposition to the policies of the US government, including speaking, writing, political demonstrations, even the filing of legal briefs.

The *Times* report comes only three days after FBI raids on

antiwar political activists in Minneapolis and Chicago, who could face charges of providing "material support" for terrorist organizations because they have spoken and written in opposition to US foreign policy in the Middle East and in Colombia.

According to an attorney for one of those targeted, the dragnet was so all-encompassing that FBI agents seized "any documents containing the word Palestine."

By the same logic, any data packet passing through the Internet with the word "Palestine" could be subject to interception, decryption, and storage in a federal database where both the person sending the message and the person receiving it would be permanently recorded as under suspicion of links to terrorism. Other words suggest themselves as likely targets: socialism, class struggle, imperialism, revolution, Marxism, Trotskyism.

The US national security apparatus seeks the power not only to spy on the Internet, but to seize or shut it down entirely when that might seem advantageous. Former CIA director Michael Hayden, interviewed by Reuters at a cyber-security conference in San Antonio, Texas on Sunday, called for giving President Obama, or any president, the power to shut down the Internet. "It is probably wise to legislate some authority to the president to take emergency measures for limited periods of time, with clear reporting to Congress, when he feels as if he has to," he said.

Hayden was echoing a view that is increasingly widespread in official Washington. In June, a Senate subcommittee approved a bill, introduced by Joseph Lieberman, the right-wing Democrat from Connecticut, declaring the entire World Wide Web a "national asset" of the United States and giving the president the power to seize control of the Internet or order its complete shutdown "for national security reasons."

The 197-page bill is entitled "Protecting Cyberspace as a National Asset Act," or PCNAA. It has the backing of another top Senate Democrat, Jay Rockefeller of West Virginia. Big software companies and Internet Service Providers (ISPs) are supporting the bill because it grants them immunity against civil lawsuits for any damage caused by a shutdown or government takeover.

Also on Monday, the US Treasury Department issued proposed new regulations that would require American banks to report all electronic money transfers into and out of the United States, regardless of the amount. Up to now, transfers of $10,000 or more had to be reported.

The new regulations were issued under the Intelligence Reform and Terrorism Prevention Act, passed in 2004, which gave the treasury secretary authority to require such reports to "combat terrorist financing." The new rules would require banks to pump information on 750 million transfers a year into a huge new database that could be mined by police, intelligence and regulatory agencies.

The information accompanying a wire transfer usually includes the name, address and account number of sender and recipient, as well as identification such as a driver's license or passport number if required by the money service. Banks would have to provide Social Security numbers for senders and recipients on an annual basis.

These actions demonstrate that a turning point has been reached in the erosion of democratic rights in the United States. A full decade ago, at the time of the stolen presidential election of 2000 and the Supreme Court's anti-democratic decision in Bush v. Gore, the Socialist Equality Party and the *World Socialist Web Site* warned that there was no longer any constituency for the defense of democratic rights within the American ruling class.

For a decade since the 9/11 terrorist attacks, first under Bush, now under Obama, the American ruling class has erected the framework for a police state. At no stage in this process has there been any significant opposition from any section of the political establishment.

Now the United States stands on the brink of major social struggles, with tens of millions of working people seeking the means to fight to defend jobs, living standards and public services. The American ruling class has long understood that the real threat to its vast wealth and privilege comes not from foreign "terrorists," but from below, from the working people who constitute the vast majority of the population.

Working people must be equally clear-eyed: millions will now come into conflict with the vast military/intelligence apparatus of the federal government. What is posed now is a turn to political struggle, to the independent political mobilization of the working class against the two official parties of big business, the Democrats and Republicans, and against the capitalist state itself.