theguardian

Internet companies warn over government email surveillance plans

Firms concerned that coalition's proposals to monitor email and social media could be misused by autocratic regimes

Josh Halliday
guardian.co.uk, Monday 2 April 2012 16.37 BST
Article history

Internet firms have warned that proposed government powers to monitor public emails could be misused by autocratic regimes. Photograph: Alamy

Internet companies have warned that the government's plans to monitor email and social media use by the British public could be used by autocratic regimes to justify state surveillance.

No internet businesses were willing to mount a public criticism of the coalition's controversial plans on Monday, but many privately raised fears over the power of authorities to see who is contacting whom online in real time.

"There is a question of jurisdiction. There is a risk that if you offer this access to Britain then you have to offer it to countries like Syria and Bahrain," said an internet industry official who declined to be identified because the proposals have not been outlined in detail.

The fears follow strong criticism from a number of MPs and civil liberties groups who argue that the plans will endanger privacy and unfettered free expression online.

Julian Huppert, the Lib Dem MP, said on Twitter that the Commons home affairs committee wanted to call the home secretary, Theresa May, to give evidence on the proposals. More than 14,000 people signed a petition by the internet advocacy body Open Rights Group against the plans on Monday.

The coalition's proposals, expected to be outlined in the Queen's speech on 9 May, will allow the authorities to have "on demand" access to online communication in real time.

However, the security minister James Brokenshire said the emphasis was on solving crime rather than "real-time snooping on everybody's emails".

He told BBC Radio 4's World at One programme: "We absolutely get the need for appropriate safeguards and for appropriate protections to be put in place around any changes that might come forward. What this is not is the previous government's plan of creating some sort of great big Big Brother database. That is precisely not what this is looking at."

One official familiar with the plans said the government wanted to bring social networks, such as Twitter and Facebook, "broadly into line" with existing legislation covering the surveillance of phone calls. Authorities would not be able to read the content of messages without an intercept warrant issued by the home secretary.

The Home Office is understood to have outlined its plans at a meeting in January with the Internet Service Providers' Association (ISPA), which represents companies including Google and BT, after a series of high-level meetings with the government intelligence agency GCHQ.

No detailed proposals have been seen by ISPA. The body was given only a cursory outline of what the government hopes to introduce.

Internet companies are anxious to learn what they will be required to do under the bolstered surveillance law. Internet service providers, such as BT and TalkTalk, could be required to install systems to harvest so-called packet data from internet communications, meaning security officials will be able to see who is visiting which websites and talking to whom.

"We haven't seen full proposals yet and we are hoping for more information from the Home Office soon … It appears to be something we would have to look very carefully at," said one industry official.

Another official suggested that stronger powers to secretly monitor internet communication could compromise the government's bid for transparency.

But the backlash over the plans has been capitalised on by some internet firms. Tor, the internet anonymity shield used by activists in Iran and China, said it would support users who wished to evade detection by UK authorities.

Andrew Lewman, the director of Tor, compared the Home Office plans with data retention laws in Germany that require internet providers to log the website visits of each user. He said use of Tor rose dramatically after that law was introduced.

"Once the data is collected, regardless of the current intentions, it will be used for all sorts of reasons over time," Lewman told the Guardian. "The number of crimes will expand to include all sorts of petty issues, political repression, and restrictions on speech. Eventually someone will think they can predict crime before it happens by using the data."

The Association of Chief Police Officers (ACPO) said the impact of communications data on criminal investigations was "critical to the ability of the police service to protect the public".

A spokeswoman for ACPO said: "Telecommunications technology is changing rapidly and in this new world there is a need to look at how we can ensure the capability to investigate crime, save lives and prosecute offenders is maintained.

"It is a matter for government to ensure the right boundaries are set so that our approaches are justified, necessary and proportionate."