Email spying: Gillard’s croc of Stalinist totalitarianism

by Kismo *Sunday, Apr 13 2008, 8:40pm*
international / human rights / commentary

> The totalitarian leaning Australian government announced today that it would legislate to allow ‘employers/bosses’ to read the emails and other digital communications of their employees. A ‘slight’ intrusion on personal liberties to say the bloody least – perhaps staff should read managements’ emails to maintain a security balance! Who is watching the watchers? No one of course! This strategy is unadulterated totalitarian poison, designed to alienate and engender mistrust and division among employees and make them more amenable to their employer’s control. The feeble excuse offered the Australian public for this unacceptable intrusion is maintaining “national security.” Not so, Ms Stasi Gillard!

Deputy PM and former card carrying 'red', Julia Gillard

IT security is a highly specialised field; intrusion detection is beyond the skill level of almost all employers/bosses, so their interest is pure snooping and employee intimidation! Expert security consultants command an average of $500/hour and up to $5000/hour for critical security troubleshooting, how many average bosses could afford or would be willing to pay these rates and what exactly are they looking for, Ms Gillard? Malicious code is beyond their feeble understanding?

Malicious attacks on networks are varied both in purpose and scope; from surreptitious data theft to overt distributed denial of service (DDoS) attacks and everything in between. Regardless of the type of external attack it would be highly unlikely that a functional connection could be made to an employees personal email, which should have been automatically scanned prior to reaching the client. It should be noted that your average email scanning software automatically detects viruses, trojans, and an assortment of other malicious code. There is absolutely no valid reason for unqualified persons to ‘read’ personal email content!

In the event that real terrorists are communicating by email, they would obviously utilise (unreadable) encryption and/or simple coded language and everyday expressions to denote other articles or meanings – so what is your real INTENT Ms Stalin Gillard?

Network monitoring software has existed for over 20 years; it is a simple matter to click on any node in a network and watch in real time (on your screen) exactly what appears on the screen of the remote node. However, this type of intrusive monitoring does not extend to reading the content of emails.

Gillard’s attempt to serve the interests of corporate bosses -- who bitterly complain that employees are constantly accessing social networking sites during work hours -- is transparent. Restricting access to the internet is a simple remedy! Average IT consultants are easily able to tailor LANs and WANs to suit client needs. That is their bloody job, not snooping into peoples’ private lives!

Gillard’s “national security” excuse is ridiculous and is reminiscent of the illegal internal surveillance the Bush regime conducts on its own citizens. It appears that Kevin Rudd picked up some very bad habits during his visits to Washington and Beijing!

Security agencies have installed and utilise huge scanning systems around the world, including Pine Gap and a new installation in Northern Australia. These installations scour the entire digital world of communications for trigger phrases and keywords – ‘echelon’ and ‘carnivore’ are the most widely known systems. This practice is decades old. Combined with content filtering at provider (ISP) level, recently introduced by the Australian ‘Labor’ government, accessing the content of personal email communications is unwarranted and completely unjustifiable!

The most vulnerable area of computing today is commercial software packages, applications and Operating Systems, especially Microsoft products! If Gillard truly wishes to tighten security she should start with implementing robust, Open Source software in all sensitive working environments and institute penalties for software vendors that produce faulty products.

http://www.smh.com.au/articles/2008/04/13/1208024990775.html

Cleaves Alternative News. http://cleaves.lingama.net/news/story-1013.html