Big Brother is Not on His Way - He's Been Here All Along

Geert Kampschoer

A topic that is capturing the imagination of both the business world and the public at large at present is the UK *Regulatory of Investigatory Powers* (RIP) Bill that was recently passed as an Act of Parliament. Geert Kampschoer, Wellance Chief Executive Officer, offers his views as to why the RIP Bill is by far not the most alarming security concern for Internet users.

At the end of the day, the 'Regulation of Investigatory Powers' bill is designed to protect us by allowing the security services to proactively police the Internet and to uncover its use in illegal and often gut-wrenching activities, like being the glue for paedophile rings. To do this effectively, the Government will monitor information exchanged over the Internet. The Bill's underlying principles are fairly clear. ISP's operating in the UK will have to provide the security services in connection with access to their e-mail traffic. However, the monitoring body will only lawfully be able to make use of that access once it is in possession of a warrant. This will be granted when certain criteria are met, criteria that are unlikely to differ greatly from the criteria that have to be satisfied for search warrants to be granted by a court of law. Yet, whilst the latter are commonly accepted, there are people all over the UK up in arms over the RIP Bill.

At the cost of sounding controversial, I am somewhat amused by this uproar - amused and concerned. It would appear as if the RIP Bill is set to dramatically alter the current state of affairs, to render e-mail an insecure, unreliable means of communication. But the truth of the matter is that e-mail is an insecure and unreliable means of communication anyway. At this very moment, thousands upon thousands of confidential documents are floating around in the ether, open to all sorts of breaches and prying eyes. Senders and recipients should be concerned, since it would be a mistake to assume that documents and information traveling over the Internet are for their eyes only. We all know that the contents of an envelope or even of a telephone call are not immune from inspection from a variety of quarters. The fact that communications should be for our eyes or ears only is a leap of faith that is actually very naïve.

This new aspect of Big Brother has stirred all sorts of emotions - anger, offence, mistrust... Yet the RIP Bill allows the Government to monitor e-mail traffic. If we, the users, can trust anybody, surely that is the Government? After all, we don't seem too concerned about the fact that hackers all over the world may be reading our sales reports, our quotes, our budgets or even sending us lethal viruses. So why should the Government be such a threat; why should we see this as yet another aspect of Big Brotherdom?

What the Bill has done, however, is to reiterate why business users need to think beyond the Internet to establish a foundation for serious Internet-based communications, especially in this new networked economy. Do not be fooled - e-mail is an unsatisfactory means of communication for people who are serious about e-business. It does not provide any management control, the status of sent e-mails cannot be monitored, and it's nigh on impossible to confirm who has read it or even who has refused it. So users are not in control of outbound communications because they cannot monitor and audit them. Basically, e-mail is a chink in your overall security. To use the Internet seriously for an ebusiness strategy, you've got to protect much more than you might at first think - the RIP Bill is bringing this lack of security in to focus.

But that doesn't mean that secure e-business cannot be a reality. It can, and should, because a totally safe environment for doing business transactions across the Internet is available. By the same token, there is no reason why you cannot provide additional value to your supply chain by making it impenetrable from prying eyes - even if they belong to the Government. There are services out there that help to make the Internet secure. However, it is wise to be vigilant, since many of these services rely upon 128-bit encryption techniques i.e. PKI (public key infrastructure). Also PKI software only provides a secure means of transmitting and encrypting information. Consequently, using it gives user organisations a false sense of security, as it is very limited in its scope to provide absolute protection. It is like putting soldiers into an impenetrable tank, crossing the battle-field unscathed despite the many attempts to blow it up, arriving and releasing the soldiers at the final destination - only to have them shot down in flames as they step our of the security of the tank. PKI helps guarantee a secure journey, not a secure destination. Moreover, it does not address the issue of control over Internet-based communications.

To date, there are only a limited number of services available designed to go beyond PKI to offer a managed and controlled environment. Amongst those offering Internet security services that go beyond PKI are Tumbleweed, PrivateExpress and Wellance. Regedoc from Wellance works via a *private* key infrastructure which is extremely difficult to break because the key is held by the individual and not awarded by the ISP, as is the case with the *public* key infrastructure. In addition, services should also offer complete control and management capabilities, allowing users to trace and track distribution of information, offer confirmation of receipt with date and time stamping and electronic signature.

It is this level of detail that will enable e-documents to become evidential in courts of law. In the face of the RIP bill, such services offer a different perspective as users retain control and privacy. For example, for the Government to view documents being managed by a service of this type requires the securing of a warrant

to approach the sender and/or recipient for access. This is not the case with straightforward PKI, where ISP's can still intercept and hand over content without the knowledge or consent of the 'owner'. While it is true that further enquiries require a warrant to be served upon the 'company', one of the main worries seems to be that the Government's security services are free to snoop. Perhaps more damning is that, under the legislation, an ISP is not obliged to inform the end user of any Government intervention.

So in this networked world where we all expect to conduct business electronically, it is imperative that the communication services we use are as resistant to penetration as possible. To provide both sender and recipient with the comfort and lasting proof of the information's integrity is a crucial business need that must be addressed. Today this is only possible via technological advancements such as non-repudiation, time and date stamping, private key encryption and, of course, digital signatures.

So while the RIP Bill has caused quite a furore, it never was about crippling business - it is about catching criminals in the act. If business is really concerned about security, it should look a little closer to home at some of the real threats to its confidentiality when using the public Internet. Big Brother is not being let in by the RIP Bill - he's been around for a while. In fact, he might be reading that report you sent off last week as you come to the end of this article. Do you still feel in control of your communications - and your business?