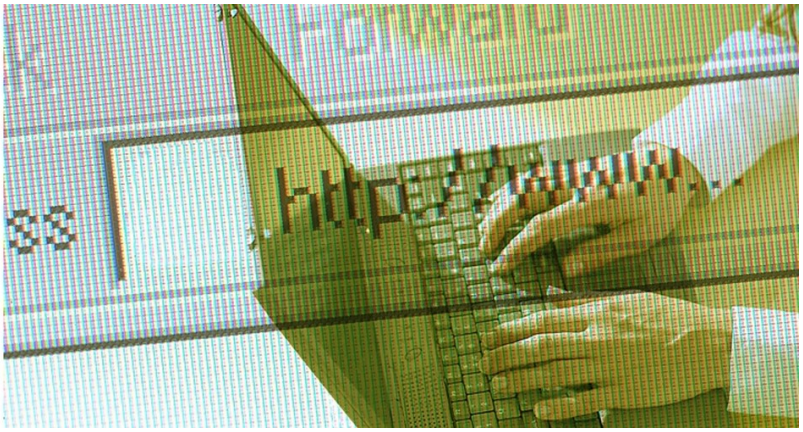
Written by **C. Mitchell Shaw** on November 6, 2014

British Spy Chief Claims Internet Services Aid Terrorists, Need More Monitoring



British spy chief Robert Hannigan has called Internet services such as Twitter, Facebook, WhatsApp, and others "the command-and-control networks of choice for terrorists" and says he wants "better arrangements" with tech companies for the surveillance GCHQ (the U.K. equivalent of the NSA) conducts on those who use these services. Considering the large amount of information GCHQ and other Five Eyes agencies already scoop up, one is left to wonder what "better arrangement" he could want. Eva Galperin of the Electronic Frontier Foundation was quoted by BBC News as saying, "GCHQ is responsible for what has come out in the Snowden files as the largest internet surveillance programme we have found to date. Their powers are already immense. I think asking for more is really quite disingenuous."

Hannigan's op/ed article, published online by *Financial Times* his first week on the job, accuses technology companies of being in denial over the way the Internet is misused by terrorists and of being out of sync with those who use the Internet for legitimate purposes. "To those of us who have to tackle the depressing end of human behaviour on the internet, it can seem that some technology companies are in denial about its misuse. I suspect most ordinary users of the internet are ahead of them.… I think those customers would be comfortable with a better, more sustainable relationship between the agencies and the technology companies." This does not appear to be the case, however. In an ironic twist, *Financial Times* posted a poll right beside his article asking, "Should online privacy be sacrificed to combat terrorism? The "Nos" outnumber the "Yeses" by a margin of more than two to one.

Many had hoped that the new director of the British spy agency would address the scandal of the Snowden revelations with reform. They are now disappointed to see him, instead, come out swinging a bigger stick than his predecessor. Julian Huppert voiced this disappointment in an article on *The Guardian's* website. "One might expect Hannigan to begin his new post on a conciliatory note — recognising the need for reform and reaching out to the public. But his article does precisely the opposite. In an extremely controversial piece, he instead blames digital companies such as Twitter, Google and Facebook for the ills of the world. He has chosen to attack people who are rightly concerned about people's civil liberties in this digital age." Glyn Moody, writing for *Computer World UK*, called Hannigan's article "a cynical, misleading and deeply-worrying assault on the Internet and its leading companies." Apparently, reform is not coming any time soon.

The basis for Hannigan's accusations is found in his assertion that "Isis has embraced the web as a

noisy channel in which to promote itself, intimidate people, and radicalise new recruits." It does this, he says, using "messaging and social media services such as Twitter, Facebook and WhatsApp, and a language their peers understand." The problem is compounded, according to Hannigan, by the encryption available that allows greater security of communications. "Terrorists have always found ways of hiding their operations. But today mobile technology and smartphones have increased the options available exponentially. Techniques for encrypting messages or making them anonymous which were once the preserve of the most sophisticated criminals or nation states now come as standard. These are supplemented by freely available programs and apps adding extra layers of security, many of them proudly advertising that they are 'Snowden approved.'" The implication is that only people who have something to hide would use these tools to secure their e-mails, texts, phone calls, and other communications. The reality is that these tools are used by millions of the "ordinary users of the internet" Hannigan appeals to when calling for even more power to digitally spy on terrorists and the rest of us.

Hannigan is guilty of pitting security against privacy, as if they are mutually exclusive. In reality, when there is greater privacy and liberty, there is greater security. The "better arrangement" he seeks would make us all less secure by making us less free in the area of privacy. Over the past several years, hackers (both criminal and government) have used the vulnerabilities created by these types of "arrangements" to compromise computer systems of governments, companies, and individuals. Computer security expert Bruce Schneier wrote for CNN.com, "You can't build a 'back door' that only the good guys can walk through. Encryption protects against cybercriminals, industrial competitors, the Chinese secret police and the FBI. You're either vulnerable to eavesdropping by any of them, or you're secure from eavesdropping from all of them." He offers a list of real-life instances of hackers using these exploits to gain information and control of systems they would not have been able to otherwise.

Fortunately, at least some technology companies seem to understand this. A tech industry group that represents 860 tech companies in the U.K. has rejected Hannigan's deal. Julian David, CEO of techUK was reported in *The Telegraph* as saying, "Any obligations placed upon technology companies must be based upon a clear and transparent legal framework and effective oversight rather than, as suggested, a deal between the industry and government." Not surprisingly, both Apple and Google, who both recently announced better encryption out of the box are represented in this rejection by techUK.

It is Hannigan who appears to be out of sync with "most ordinary users of the internet." While saying he is open to "public debate about privacy," he shows his true attitude toward privacy by writing, "For our part, intelligence agencies such as GCHQ need to enter the public debate about privacy. I think we have a good story to tell. We need to show how we are accountable for the data we use to protect people, just as the private sector is increasingly under pressure to show how it filters and sells its customers' data. GCHQ is happy to be part of a mature debate on privacy in the digital age. But privacy has never been an absolute right and the debate about this should not become a reason for postponing urgent and difficult decisions."