

Better locks to secure our data are the inevitable result of too many prying eyes

November 5, 2014 11.21am GMT



Author



Bill Buchanan

Head, Centre for Distributed Computing,
Networks and Security, Edinburgh Napier
University

It was bound to happen eventually. wk1003mike/Shutterstock

Robert Hannigan, the new head of British signals intelligence agency GCHQ, has accused technology companies of aiding terrorists and criminals by providing them secure communications through their products and networks.

Far from adopting a conciliatory tone following last year's revelations from documents leaked by Edward Snowden about government spying on citizens, the intelligence chief has doubled down, railing against companies like Microsoft, Google, Facebook, Yahoo and Apple for what some will see as trying to balance user privacy against the rapacious demands of the surveillance services.

Hannigan's statement is bound to rile some. Privacy, he says, has never been "an absolute right". Extremist groups are using the liberties granted them by the web: while some have been harboured by dark areas of the net in the past, ISIS instead uses the internet to openly "promote itself, intimidate people, and radicalise new recruits."

Last month Apple released iOS 8, the latest version of its mobile phone and tablet operating system, with encryption for the phones contents enabled by default. This led to outcries from the FBI that it would make their work harder, while a Chicago police chief claimed the iPhone would become to “choice of phone for paedophiles”.

The fifth version of Google’s Android operating system, codenamed Lollipop, is released next week with similar security upgrades. Besieged by thefts and leaks of anything from intimate photos to financial data, users might legitimately ask why it has taken so long.

The protection for digital files on computers or phones provided by file attributes and content types has barely changed in decades, and is based on concepts of stand-alone computer systems, and with little thought on keeping things truly private. This works well from a corporate point of view, where we can keep backwards compatability and allow IT department administrators to keep full control.


The firms creating mobile devices, however, have different issues, as their devices are on the move, and often stolen or mislaid. The internet itself is built from the protocols used in the days of mainframe computers and teletype terminals, with little thought given to protecting data as it is stored and transmitted. Now more connected, more mobile than ever, we carry our most sensitive data with us all the time: what was once protected by firewalls and physical security is now in our pocket.

With mobile phones increasingly integrated into our lives, the devices need to be more protected than our traditional desktop computers. So Apple and Google now find themselves with consumers who will switch mobile devices to keep up to date, without many decades of previous operating systems and application software to maintain compatibility with – the ball and chain around Microsoft’s neck, particularly. With the power and speed of even mobile phone hardware now considerable and growing all the time, the days when a special maths chip was needed to perform complex cryptography are gone.

This tension between law enforcement and the right to privacy remains unresolved. The FBI currently see the status quo, where major tech companies are persuaded or brow-beaten into cooperating with police and security agencies under the PATRIOT Act, as necessary to pursue criminals and terrorists. In the UK the Regulation of Investigatory Powers Act 2000 (RIPA) defines what information of citizens that law enforcement can access, with the support of a warrant.

In both cases this will undoubtedly become harder with encryption-by-default, and the same tension exists with encrypted and anonymised “dark net” service Tor, where law enforcement are scared that crime can go un-noticed, whereas privacy advocates promote the privacy capabilities it offers. But the introduction of improved security is a predictable response to a situation in which the agencies headed by Hannigan’s predecessors and fellow spooks have been seen to ease themselves past those

safeguards to citizens' information that remain.

 [Online privacy](#) [Surveillance](#) [GCHQ](#) [MI5](#)