

Academic rigour, journalistic flair

Arts + Culture Business + Economy Education Environment + Energy Health + Medicine Politics + Society **Science + Technology** Election 2015

Follow Topics Rosetta Explainer Digital economy Hubble 25 LHC Ceres

5 November 2014, 11.21am GMT

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

AUTHOR



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

DISCLOSURE STATEMENT

Bill Buchanan does not work for, consult to, own shares in or receive funding from any company or organisation that would benefit from this article, and has no relevant affiliations.



It was bound to happen eventually. wk1003mike/Shutterstock

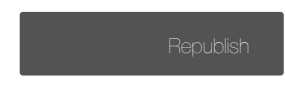
Robert Hannigan, the new head of British signals intelligence agency GCHQ, **has accused technology companies** of aiding terrorists and criminals by providing them secure communications through their products and networks.

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

REPUBLISH THIS ARTICLE

We believe in the free flow of information. We use a **Creative Commons Attribution NoDerivatives** license, so you can republish our articles for free, online or in print.



SHARE

Email Twitter



Provides funding as a Member of The Conversation UK.
napier.ac.uk/Pages/home.aspx

EDINBURGH NAPIER UNIVERSITY EVENTS

Are we really safe? Ñ Edinburgh

MORE EVENTS

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 the 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 compatibility 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

Facebook 2

LinkedIn 23

Reddit

Sign in to Favourite

2 Comments

Print

TAGS

Online privacy, Surveillance, GCHQ, MI6

ARTICLES BY THIS AUTHOR

24 February 2015
Lenovo's security debacle reveals blurred boundary between adware and malware

22 January 2015
If Obama is talking about securing the net, it should be on everyone else's lips too

14 January 2015
If you seek to switch off encryption, you may as well switch off the whole internet

24 November 2014
Codebreaking has moved on since Turing's day, with dangerous implications

31 October 2014
In cybersecurity, the weakest link is É you

RELATED ARTICLES

Making ISPs enforce age checks for porn puts responsibility where it might actually count

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.

Spying on your kid's phone with Teensafe will only undermine trust

What use would a digital bill of rights be?

Online and out there: how children view privacy differently from adults

SHARE

Email

Twitter 10

Facebook 2

LinkedIn 23

Reddit

Like us on Facebook

Follow us on Twitter

Sign up to our free daily newsletter

United Kingdom

Join the conversation

Sign in to comment

2 comments sorted by

Oldest

Newest



David Wright

logged in via email @gmail.com

Private companies are not and should not be arms of government agencies. I see no

attempts to keep criminals off freeway systems; the analogy is the internet as a digital freeway. I do not trust, and actually loathe, the 'security services'. They make me less, not more, secure. I trust terrorists in the sense that I can predict what they'll try to do, and even how. Also, what they do is what they say they'll do! What government follows this path, or is so honest or direct? None I know of. Washington and London in particular, as they're the ones of which I have most experience.

Contra the sainted Marshall McLuhan (does anyone under 60 remember him?) the medium (internet) is NOT the message. Stop treating it as if it were.

6 months ago [report](#)



Peter Houpermans

logged in via email @phx.li

The physical equivalent of weakening crypto in order to protect us "better" is to ask everyone to install easy to pick locks in their backdoors and offer vague assurances that only the "right" people will use that.

I'm curious: how would these people secure Fort Knox? Install a Labrador-sized dog flap in the back?

6 months ago [report](#)

THE CONVERSATION

Community

[Community standards](#)

[Republishing guidelines](#)

[Research and Expert Database](#)

[Events](#)

[Our feeds](#)

Company

[Who we are](#)

[Our charter](#)

[Our team](#)

[Our blog](#)

[Partners and funders](#)

[Contributing institutions](#)

[Contact us](#)

Contact

Editorial uk-editorial@theconversation.com

Support support@theconversation.com

Subscribe to our Newsletters

United Kingdom