FINANCIAL TIMES

Click here to try **our new website** — you can come back at any time

December 17, 2015 6:21 pm

The hype over metadata is a dangerous myth

Thomas Rid

Share Author alerts Print Clip Gift Article Comments

The UK risks setting a worrying precedent for more illiberal jurisdictions, writes Thomas Rid

©iStock

Communications data — and the government's powers to collect them — are at the heart of the draft Investigatory Powers Bill introduced by Theresa May, UK home secretary, which is currently under scrutiny.

Such metadata are the digital exhaust of our phones and laptops, the "who, where, when, how — and with whom" of our chatty online selves. These data are a live issue worldwide. In the words of a former general counsel at the US National Security Agency, Stewart Baker: "Metadata absolutely tells you everything about somebody's life."

But is this tool really so powerful in the hands of the police and intelligence agencies? In practice the importance of bulk data, contrary to "big data" hype, has been shrinking in recent years. Our familiarity with letters, phone calls and good old emails has duped us into thinking that metadata are highly revealing — often they are not.

The first reason is the rise of encryption. Almost all Google's services have been encrypted since 2011. Facebook started in July 2013; Yahoo in 2014. The messaging app WhatsApp is encrypted. So are Twitter, Amazon, eBay, Wikipedia, your bank and the UK government's pages, with the US government not far behind. Users do not have to do anything. Encryption is on by default.

One consequence is that interceptable metadata become truncated, in a way akin to removing the name and house number from a letter. Encrypted data "packets" only contain two so-called IP addresses — the often temporary but crucial calling number of every internet device — and do not show the revealing details displayed in the browser address bar. In short, connections built into most popular internet sites do not reveal if somebody is looking at cat clips or messaging with a militant.

People are also using far fewer metadata-spewing phone calls and emails; millennials often use messaging apps instead. And the bulk data of most encrypted internet communications do not reveal who is talking to whom. The data do reveal the name of two organisations, for instance a platform provider, say Facebook, and a user's internet service provider, say BT. Linking one IP address to an individual person requires the co-operation of BT; linking two IP addresses together as the two ends of a conversation requires the co-operation of Facebook. Developing metadata, in short, often requires warrants and more digging.

Another recent trend is the rise of permanent connections for messaging. Phone metadata are useful because we are not talking to everybody all the time. But many users are logged into messaging accounts all day, with push notifications on. Timing is crucial for metadata but permanent sessions often mean timing is practically meaningless.

Connections built into most popular internet sites do not reveal if somebody is looking at cat clips or messaging with a militant

Then there is the rise of technologies purpose-built to hide the user. Tor, for example, is an anonymity network, and its opaque design means there is no trusted "third party" where law enforcement could even present a warrant. Blocking such tools is technically difficult and politically unacceptable for a liberal democracy.

The erosion of communications data will continue, as previously hard-to-use security software becomes easier to navigate and is more widely adopted.

Metadata are still useful for unearthing targets. After a terrorist incident, for instance, stored data can be crucial in order to reconstruct events and exploit intelligence — not unlike CCTV.

Yet overestimating metadata, as many do, is dangerous in two ways, one practical, one political. The practical danger is that the government is antagonising Silicon Valley developers by clinging to a blunted counterterrorism tool. The political problem is linked to that business issue: seduced by the metadata myth, the Home Office has muddled the message on encryption. The Investigatory Powers Bill, in its current form, reiterates an outdated and legally untested status quo that could allow the government to force companies to remove specific forms of end-to-end encryption.

Senior officials, in closed-door meetings, have indicated repeatedly — and unrealistically — that the bill would “restore lost capabilities”. The Home Office, in other words, may ultimately test this power in court. Such a move would incur large political costs for very little security benefit. Apple, Google and others rightly fear that the UK risks setting a dangerous precedent for more illiberal jurisdictions, in Europe and especially in China. The White House, for now, has decided not to seek legislation that limits encryption. It is time for Whitehall to drop the implicit encryption provisions from its bill. By doing so it would reaffirm the UK’s prime spot among the world’s liberal democracies.

The writer is an academic and author of the forthcoming ‘Rise of the Machines’

RELATED TOPICS Cyber Security, United Kingdom, UK infrastructure, Data protection, UK Broadband

Share Author alerts Print Clip Gift Article Comments

Printed from: http://www.ft.com/cms/s/0/e0da1c64-a4b5-11e5-a91e-162b86790c58.html