FREELANCE

Hacks vs. spooks

VETERAN security affairs reporter Duncan Campbell and Professor Ross Anderson discussed at May’s London Freelance Branch meeting the Investigatory Powers Bill still before parliament – and “tradecraft” for journalists wanting to protect the anonymity of our sources in this digital age. (See the bottom of this page for their tradecraft advice.)

Ross Anderson, Professor of Security Engineering at the University of Cambridge and an expert on computer communications, reminded us that surveillance and revealing confidential sources affect everybody doing investigation, not just journalists.

Duncan Campbell opened by saying how he was “struck by the pivotal role of the National Union of Journalists in protecting journalism, journalists and freedom of expression”. He recalled how he, his colleague the late Crispin Aubrey and a source, ex-soldier John Berry, had been arrested under the Official Secrets Act in 1976. The resistance started at an NUJ Delegate Meeting “in the sands of Whitley”, as NUJ members stamped out the name of a secret witness against them on the beach. Later four MPs, including NUJ members, spoke the sacred name during Prime Minister’s Questions.

The current Investigatory Powers Bill now before Parliament is a Something Must Be Done Law whose purpose, said Ross, is to “make legal a lot of the dodgy things that (US National Security Agency whistleblower) Ed Snowden told us that [spook HQ] GCHQ were up to”.

Ross flagged some of the Bill’s provisions. National Service providers (ISPs) will be compelled to keep records of what websites you’ve connected to. Also included are warrants for equipment interference – see below – and powers to “compel assistance”. Rather than threatening a journalist with jail unless they reveal their source, the state could instead threaten their ISP, which is much more likely to fold.

Now security services looking for leakers don’t need to arrest MPs or search their offices – they can just do a “snowball search” – using that who-called-who “metadata” to trace the contacts of a target’s contacts and so on. Even if a target hadn’t talked to his source directly, just “two layers out” they’d find that he’d called Fred Smith, and two minutes later Smith had called Jones… who would be under suspicion.

GCHQ now have cheap access to all your calls and text messages but also for email and other channels, records of who visited a website – and everyone else visiting the same site – and so on. Snowden’s leaks demonstrated that when past efforts at legislation to legitimise this, initiated by Home Secretaries Jacqui Smith and Teresa May, fell, GCHQ went ahead and did it anyway.

The Investigatory Powers Bill includes granting warrants for “equipment interference”. Ross says it’s possible to “hack the emergency assist button in a car” and described a case where the talking Barbie doll of a suspected gangster’s granddaught er, relaying everything in the room.

PRECAUTIONS to protect our sources in the digital age were on the agenda at May’s LFB meeting. Speaking on the subject were Duncan Campbell and Professor Ross Anderson (see above).

Our sources, said Ross, need to be able to contact us in the knowledge that they will not be prosecuted or persecuted, and without leaving a trace. Consider letting them know what pubs you can be found in, when, rather than giving a specific time and place. We need to think about the “shoe-leather stuff” – making sure we’re not followed there.

Ross was once contacted by a missionary in Texas about communicating with converts to Christianity in Pakistan – where converting is a capital offence. How could he communicating with then, safely? PGP encryption on emails? Or Skype? Millions use Skype and few use PGP. The authorities can easily trace everyone who uses PGP – “anonymity lies only in the technicalities, but it stands out. Meeting your contact at 3am in Trafalgar Square is not a good idea; 3pm is.

Do not put your faith in technical fixes. Some people have built special systems for whistleblower communication. Being found to use such a system will draw attention to anyone, who “will be in manacles by dinner time”.

Duncan reinforced the message of tradecraft trumping technical fixes. “If your source is a nurse they need reassurance, and they do not need to be asked to install some gizmo.”

If you’re dealing with a really serious case, keep a computer specially for that case – one that is “airgapped”, never connected to the internet. Consider using an operating system that fires up from a DVD, such as Tails, so that any attempt at “equipment interference” will be futile. Consider also a new phone for the same purpose (a “burner phone”). Ross said payphones are technically, but it stands out. Meet ing your contact at 3am in Trafalgar Square is not a good idea; 3pm is.

See SPOOKS on page 3

© Mike Holderness

Tradecraft for journalists in a digital age

• Can the state secretly order me to damage my neighbour’s stuff or trespass on his privacy?
• Capture of dark powers by lobbies?
• Legally, globalisation, jurisdiction, liability the real killers?
• Who will be harmed by my data?
• More: see my IPT testimony on our blog http://www.lightbluetouchpaper.org

LFB meetings
11 July
Migration, diversity
Aug – no meeting
13 September
Working with techies (tbc)
See back page & www.twitter.com/NUJ_LFB

© Mike Holderness
• There’s more via an insecure online connection at www.london-freelance.org/fl/1606ipb.html