Viewpoint

Is it time to go back to the typewriter, carbon paper and Tippex?

Tony Bunyan

The “white-washing” report on GCHQ, MI5 & MI6 by the Intelligence and Security Committee [1] published on 12 March 2015 was preceded by a draft Code of Practice "Equipment Interference” [2] to allow the UK intelligence and security agencies to “legally” access computers to gather and break encrypted codes and allow “remote access” to “interfere” with any targeted computer anywhere in the world. The deadline for comments on the Code is 20 March 2015 after which it will simply be “laid” before parliament and adopted without debate.

The response of the UK government to the wealth of evidence from the **Snowden revelations** [3] concerning GCHQ, the finding of the **Investigatory Powers Tribunal** [4] on the unlawful data exchange with the NSA, **the judgment by the Court of Justice of the European Union** [5] in April 2014 that the EU Mandatory Data Retention Directive was unlawful since it was adopted in 2006 (to which the UK was signed up) and **DRIPA 2014** [6] which legalised the gathering of IP addresses all confirm that governments are not in control of their intelligence and security agencies, that the agencies use all available technologies even if there is no legal basis, and when court judgments find against present practices the law is simply changed to make the "unlawful” “lawful"

The draft Code of Practice, published on 6 February, seeks to legalise the intelligence and security agencies having direct access to computers *inside* the UK by MI5 (the Secret Service) under the **1989 Security Service Act** [7] and *outside* the UK – in the EU and the rest of the world by GCHQ and MI6 (Secret Intelligence Service) under the **Intelligence Services Act 1994**.[8]

In effect it allows **GCHQ to continue to "spy on the world".** [9] The Code says the three agencies can:

"obtain information in pursuit of intelligence requirements"

and:

"locate and examine, remove, modify or substitute equipment hardware or software"

and this applies to:

"any interference (whether remotely or otherwise)".

The agencies will - lawfully - be able to bypass encryption to gain access to content and with whom the data has been shared. They will also have *carte blanche* to search smartphones or cameras on mobile phones and switch on microphones. In effect the agencies will have **"remote access"** to computers and be able not just to see what you have written or are writing but to delete or alter content.

The draft Code (para 1.3) refers to "other specified purposes" in the 1989 Act (MI5) and 1994 Act (GCHQ and MI6) Acts. This is a reference to the scope of the 1994 Act which is: *"(ii) in the interests of national security; (iii) for the purpose of the prevention or detection of serious crime; or (iv) for the purpose of **any criminal proceedings**"* (2.2.a, emphasis added). The reference in the 1989 Act says that MI5 shall be concerned with "preventing or detecting serious crime"(2.2.a). However, it is worth reminding ourselves that the definition of MI5's purpose is:

*"the protection of national security… and from actions intended to overthrow or **undermine parliamentary democracy by political, industrial** or violent means"* (1.2).[emphasis added]

Although the Code only refers to the intelligence and security agencies "remote access" is already being used by law enforcement agencies across the EU [10] [11] even though most EU states have no legal basis in place allowing remote access to computers – including the UK where there is no reference to this in RIPA 2000.

Introducing the draft Code the Home Office Security Minister spoke of authorising:

"techniques to identify, track and disrupt the most sophisticated targets"

which sounds suspiciously like **GCHQ's 4Ds programme** [12] to:

"Deny/Disrupt/Degrade/Deceive" targets.

The Code refers to using these new powers against terrorism and serious crime but how wide will the net be cast? The official definition of "domestic extremism", in the words of HMIC, could *"lead to protestors and protest groups with no criminal intent being considered domestic extremists by the police."* (**A review of progress made against the recommendations in HMIC's 2012 report on the national police units which provide intelligence on criminality associated with protest**) [13] and the **Taylor report: Investigation into links between Special Demonstration Squad and Home Office** [14] **w**hich has been followed on 12 March 2015 by: **Home Secretary announces statutory inquiry into undercover policing** [15] and the news that the **Special Demonstration Squad** [16] spied on the National Union of Students, Unison, the National Union of Teachers, the building workers' union UCATT, the firefighters' union FBU and the Communication Workers' Union. This follows revelations that undercover police are operating in political movements in the UK and the EU: **Secrets and lies: undercover police operations raise more questions than answers.** [17]

What guarantees are there that these new surveillance powers in the Code of Practice will only be used against terrorists and serious organised criminals and that "function creep", which has happened time and again since 2001, will not see them used against "suspects", "targets", "pre-emptive" intervention and against those seeking to

"***undermine parliamentary democracy by political, industrial… means"***? [emphasis added]

A lesson from history

So is it time to go back to the typewriter, carbon paper and Tippex? The answer is emphatically "no". To do so would drive critical thought and dissent underground. We must continue to oppose and expose every government's attacks on our privacy and liberties. We must defend and exercise our right to think, speak, write and protest. The alternative is not to act freely because of the fear we might fall foul of the "thought police" which will accelerate the slide to authoritarianism and what lays the other side of it.

On the other hand if you are minded to dust off your old typewriter it should be safe from prying eyes – but then I recall a tale Philip Agee, who wrote the best-selling **"CIA Diary: Inside the Company"**, [18] told me. When he was in France, just before he came here to finish the book, a "friend of a friend" lent him a typewriter which he later discovered was transmitting every word he wrote, so best to check for any mechanical bugs.

Tony Bunyan, Statewatch Director, comments:

"The adoption of sweeping new surveillance powers to access computer remotely should be the subject of primary legislation and not sneaked through as secondary legislation in a Code of Practice under RIPA 2000 - which itself is not limited to terrorism and serious crime but covers all crime however minor.

"Moreover recent history tells us that there is no guarantee whatsoever that these sweeping new powers will only be used against suspected terrorists and serious organised crime"

16 March 2015

References

1. http://www.statewatch.org/news/2015/mar/uk-isc-privacy-and-security-report.pdf

2. http://www.statewatch.org/news/2015/feb/uk-ho-draft-equipment-interference-code-of-practice.pdf

3. http://www.statewatch.org/eu-usa-data-surveillance.htm

4. http://www.statewatch.org/news/2015/feb/uk-ripa-liberty-judgment-6-2-15.pdf

5. http://statewatch.org/news/2014/apr/eu-ecj-data-ret-prel.pdf

6. http://www.statewatch.org/analyses/no-252-mand-ret-dripa-ripa.pdf

7. http://www.legislation.gov.uk/ukpga/1989/5/contents

8. http://www.legislation.gov.uk/ukpga/1994/13/contents

9. http://www.statewatch.org/analyses/no-244-gchq-intercept-commissioner.pdf

10. http://database.statewatch.org/article.asp?aid=30612

11. http://www.statewatch.org/analyses/no-83-remote-computer-access.pdf

12. http://www.statewatch.org/news/2015/feb/gchq-disruption.pdf

13. http://www.statewatch.org/news/2013/nov/uk-hmic-review-progress-public-order-intelligence.pdf

14. http://statewatch.org/news/2015/mar/uk-2015-03-12-sds-home-office-links-report.pdf

15. https://www.gov.uk/government/news/home-secretary-announces-statutory-inquiry-into-undercover-policing

16. http://www.mirror.co.uk/news/uk-news/police-spying-whistleblower-admits-mps-5329601

17. http://database.statewatch.org/article.asp?aid=33253

18. http://en.wikipedia.org/wiki/Philip_Agee