GlobalResearch
Center for Research on Globalization

Total Surveillance: Snooping in the United Kingdom

By Dr. Binoy Kampmark
Global Research, December 08, 2016
Region: Europe
Theme: Police State & Civil Rights

The UK-based Liberty Campaign expressed it most glumly. "The Government's new Snoopers' Charter (also known as the Investigatory Powers Bill) will allow the bulk collection of all our personal information. Who we talk to; what we say; where we are; what we look at online – everything."

Championed while she was Home Secretary, Prime Minister Theresa May has seen her wishes fulfilled. Total surveillance – and there was already a good deal of that in Britain – is coming to the country. Late last month, the Investigatory Powers Bill, known by its faux cuddly, yet sinister term the Snoopers' charter, received royal assent and became law.

The sense that something smelly was in the air was evident by the enthusiasm of the Home Secretary, Amber Rudd. This nasty bit of legislation was worthy of advertisement as protective, not detrimental, to privacy. In the surveillance stakes, Britain had every reason to be proud with this bit of "world-leading legislation" that provided "unprecedented transparency and substantial privacy protection."

After trumpeting matters of privacy and transparency, Rudd came to the essential point, using the argument that the world is a terrifying place (as it always tends to be for government): "The government is clear that, at a time of heightened security threat, it is essential our law enforcement and security and intelligence services have the power they need to keep people safe. The internet presents new opportunities for terrorists and we must ensure we have the capabilities to confront this challenge."[1]

Web and phone companies will be required to store records of websites visited by every customer for 12 months for access by the security industry, be it the police or pertinent bodies, upon the issue of warrants. This tracking does not extend to VPNs.

The warrant will be all empowering, enabling relevant security personnel to bug phones and computers. Compliance and connivance from companies is also expected, thereby coopting the private sector into undermining encryption protections. That very fact should chill companies in the business of supplying communications.

The obvious rejoinder from those favouring the Snoopers' Charter is that it is not only snooping with a purpose, but snooping with delicate, informed oversight. As ever, the error here is to institutionalise snooping by giving some sense of sagacious self-policing.

If the intelligence services have proven one thing, the desire to overstep, and overreach in zeal, is compulsive. Even the investigatory powers tribunal, charged with the task of hearing complaints against MI5, MI6 and GCHQ, noted in October that an illegal regime in tracking and obtaining data, including web and phone use, had been operating for over 17 years.

Such behaviour draws out nightmarish scenarios of inevitability: the security services will always be there to undermine in the name of Her Majesty's sacred priorities, while those with data will be there for the pilfering. "I never assumed my emails and internet activity are completely private," mused Matthew Parris darkly. "Has anyone?"[2]

The intercept warrants under the new regime, by way of example, require authorisation from the Home Minister prior to judicial review. Judges, overseen by a senior judicial officer called the Investigatory Powers Commissioner, will be responsible for that task and have the power of veto.

Such padding is all well and good, but the State rarely oversees itself competently when it comes to such concepts as the greater good. Abstracted and mysterious, that greater good trumps privacy and individual civil liberties. The lust to gather data becomes insatiable.

The war against encryption has been the central object of the May brigade for some time. Importantly, it suggests institutional corrosion of basic privacy. Under Rudd's stewardship, an attack by direct means is encouraged, despite being feather bedded by dictates of privacy.

This dysfunctional nonsense has truly given Britain a "world class" regime in surveillance that will be a model to emulate by less savoury regimes. If the Brits do it in that fashion, then why not others?

As Jim Killock of the Open Rights Group explained, Rudd was right in one sense: the IP Act was truly revolutionary in its impact. "The IP Act will have an impact that goes beyond the UK's shores. It is likely that other countries, including totalitarian regimes with poor human rights records, will use this law to justify their own intrusive surveillance powers."[3]

The idea that partial encryption and half-baked measures are possible is simply dismissed as wishful thinking by such industry pundits as Nic Scott, the UK and Ireland managing director of data security specialists Code42. "You either have encryption in place or you don't. Once you create a backdoor of law enforcement powers, you are also opening the door to other, potentially malicious parties."[4]

That backdoor has been well and truly opened, and the pool of communications data signal an open season for hackers of whatever persuasion. Goodbye Data Retention and Investigatory Powers Act 2014; welcome Orwellian state-manic insecurity and data hoovering. The only obstacle now will be the spoiling verdict of the European court of justice, if the Labour party's Tom Watson gets his way.

Dr. Binoy Kampmark was a Commonwealth Scholar at Selwyn College, Cambridge. He lectures at RMIT University, Melbourne. Email: bkampmark@gmail.com

Notes:
[1]
https://www.theguardian.com/world/2016/nov/29/snoopers-charter-bill-becomes-law-extending-uk-state-surveillance
[2]
http://www.spectator.co.uk/2015/06/my-dirty-secret-i-dont-care-either-way-about-state-surveillance/
[3]
https://www.theguardian.com/world/2016/nov/29/snoopers-charter-bill-becomes-law-extending-uk-st

ate-surveillance
[4]
http://www.computerworlduk.com/security/draft-investigatory-powers-bill-what-you-need-know-3629116/

Articles by: Dr. Binoy Kampmark