“Data Retention,” Australia’s Keystone Cops and Major Party Sell-outs

by Binoy Kampmark via sally - Global Research *Tuesday, Mar 31 2015, 10:31pm*
international / prose / post

> *The first very revealing indicator of political non-representation is that BOTH major puppet parties passed this Bill into Law without adequate scrutiny or at least some proof that this Bill prevents crime. I refer to the recent Martin Place seige as evidence of a complete failure by police and other regulatory agencies to prevent a criminal action by a felon that was known and monitored by local spy agencies and the State police. And now these incompetent imbeciles have been given more material to create evermore havoc on our lives -- the details of every citizen's metadata private communications and whereabouts (GPS aware smartphones) is now readily avaialble without warrants to imbecile police and our boy scout spy agencies -- God help Oz!*

And for those citizens with media-wiped 24 hour memories, Martin Place was not the first fiasco by our clearly inept regulators. The Hilton bombing, a spy agency engineered event, which was designed to extract more funds from the government by demonstrating how our agencies saved the heads of Commonwealth Leaders at a scheduled meeting at Sydney's Hilton Hotel, ended in tragedy. As usual our idiot spys and police forgot the garbage run and hapless waste collectors were killed when the bomb, which was placed in a waste bin, was unintentionally detonated -- 'brilliant' and highly illegal. The perpetrators were never discovered, naturally, though a member of the Ananda Marga sect was fitted with the crime and later exonerated after spending years in jail.

Then there was the infamous ASIS 'terrorist exercise' designed to train its clown members in dealing with a hotel seige in Melbourne. After storming the hotel with flak-jackets and automatic weapons like a bunch of criminal school kids, hotel staff promptly called the police and havoc broke loose as idiot ASIS forgot to inform the hotel they were conducting an exercise, notwithstanding that a public hotel was a completely inappropriate arena -- I mean do I have to cite more keystone cop bungles and failed escapades? All available evidence points to the fact that the metadata will be compromised either internally or externally -- I assess facts only, not the shit that issues from the mouths of our clearly unrepresentative politicians.

So the sell-out has been achieved without a skeric of real evidence that surveilling citzens, you and me, actually prevents criminal actions and enterprises -- I refer to our FAILED gun laws which disarmed citizens but had no effect on organised crime as the recent Rose Bay spray of automatic weapons on a luxury launch indicates -- and there's more, 'grass-skirted' FOB (Pacific Islander) gangs stormed a nigh club in Oxford St Sydney and opened up with automatic weapons just like in a Hollywood movie! Naturally our agencies and police were caught flat-footed in both instances, notwithstanding the existence of dedicated gang sqauds.

So where do we go from here sheeple, as the writing is on the wall? I know but see if you can work it out for yourselves. O, sorry, did you forget that the people actually rule this country, what a shame you missed that one, you mindless, sleepwalking, paralysed mullets, you deserve everything you get!

Article by Binoy Kampmark follows:

> The Telecommunications (Interception and Access) Amendment (Data Retention) Bill

2014 is now law. Despite a few loud voices, the police state consensus barged its way through the lower house and senate. An act that is poor in terms of scope, uncertain in terms of cost ($400 billion is but a figure), and dangerous in creating unnecessary pools of data, is now part of the surveillance furniture of the Australian landscape.

While Australia forges ahead into the barren scape of policy that is data retention, other countries and institutions are finding little to merit it. The Court of Justice of the EU (CJEU) ruled in April 2014 that European Union laws requiring telecommunication providers to retain metadata for up to six months, and a maximum of twenty-four months were, in their scope and purpose, invalid as a breach of fundamental privacy rights.

Austrian and Irish applicants challenged the respective transpositions of the directive into domestic law, uncomfortable with the fact that the retained data could be used to identify the person with whom a subscriber or registered user has communicated with, and by what means; identify the time and place of the communication; and know the frequency of the communications of the subscriber or registered user with certain persons over a periods of time.

The central law in question was the EU's Data Retention Directive 2006/24(EC), which replicated, in a sense, the language of the Australian bill. Retaining traffic and location data including material necessary to identify the subscriber or user would amount to a breach of privacy and the right to protection of personal data under the Charter of Fundamental Rights of the EU.

In the Court's view, the data, "taken as a whole, may provide very precise information on the private lives of the persons whose data are retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, activities carried out, social relationships and the social environments frequented."[1] In bold emphasis, the Court argued that the data retention directive, which also enabled access by national authorities, "interferes in a particularly serious manner with the fundamental rights to respect and private life and the protection of personal data."

We could all be in some agreement, suggested the Court, about the fact that retaining data might satisfy an "objective of general interest" – the "fight against serious crime and, ultimately, public security." But notwithstanding this interest, the EU legislature had still exceeded its powers. Limits must be provided on attaining such data. The principle of "strict necessity," a point that has totally escaped officials in Canberra, is what is required. The directive, for instance, made no "differentiation, limitation or exception" to the traffic data in question.

In the United States, an eclectic grouping ranging from the American Civil Liberties Union to the World Press Freedom Committee urged the White House, Congress and the various officials in an open letter (Mar 25) to stop bulk collection as permitted by the USA PATRIOT Act section 215, including records retained under the provision and similarly section 214 covering "pen registers and trap & trace devices." In the event that these should occur, "appropriate safeguards" were to be put in place.[2]

The gods certainly do have a sense of humour. With the Australian bill still freshly passed through the upper house, it was reported that a high profile data breach had taken place before the G20 Summit in Brisbane. Passport and visa details, including date of birth of 31 international leaders were mistakenly emailed by an official in the

Immigration Department office to a member of the Asian Cup Local Organising Committee November 7th last year.[3] The Guardian Australia, after obtaining an email sent from the Immigration Department to the privacy commissioner under Freedom of Information, revealed that the breach was noted 10 minutes after the incident.[4] The Asian Cup Local Organising committee claimed to have no access to the email, or have it stored anywhere in its system.

Stunning indifference accompanied the response to what was deemed an "isolated example of human error," with minimal consequences. The then immigration minister Scott Morrison was notified, but department officials, in their wisdom, decided to stay numb on the subject. The G20 leaders would be kept in the dark.

Even by Australia's own paltry standards, this posed a serious breach. In the words the Information Commissioner, a data breach occurs "when personal information held by an agency or organisation is lost or subjected to authorised access, modification, disclosure or other misuse or interference." Australian Privacy Principle 11 imposes an obligation on agencies and organisations to take reasonable steps to protect the personal information they hold from such misuse, interference or loss, not to mention unauthorised access, modification or disclosure. With rather cheeky disdain, the Australian immigration department decided to conveniently sidestep the relevant provisions, wishing the matter to assume the form of an ostrich and vanish deep beneath the sand.

Such attitudes bode ill for the data retention program. Modification and unauthorised disclosures are genuine risks that only increase as the burdens on agencies increase. If officials of the agency dismiss the disclosure of personal details of world leaders on a summit attendance list as minor aberrations, we can only imagine how contemptuously private citizens will be treated.

Notes:

[1] http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf

[2] https://static.newamerica.org/attachments/2579-nsa-coalition-letter/NSA_coalition_letter_032515.pdf

[3] https://www.documentcloud.org/documents/1697616-g20-world-leaders-data-breach.html

[4] http://www.theguardian.com/world/2015/mar/30/personal-details-of-world-leaders-accidentally-revealed-by-g20-organisers

http://www.globalresearch.ca/data-retention-and-australias-police-state-consensus/5439830