GlobalResearch
Center for Research on Globalization

The Devotees of Data Retention and Mass Surveillance

By Dr. Binoy Kampmark
Global Research, October 09, 2022

Region: Europe, Oceania
Theme: Intelligence

***

It is a stinker in terms of policy, and unconvincing in effect, but the wholesale, indiscriminate retention of telecommunications data continues to excite legislators and law enforcement. In the European Union, countries continue to debate and pursue such measures, despite legal challenges.

The EU General Data Protection Regulation (GDPR), passed in 2016, limits the ways personal data is collected in terms of legitimate purposes. The European Court of Justice has also made it clear that the mass retention of phone and location data violates the EU's Charter of Fundamental Human Rights.

Despite this, EU member states continue to subvert, by varying degrees, such protections. Fixated by notions of protecting society from the unsavoury and the criminal, lawmakers continue to flirt and court the mass surveillance properties inherent in such regulations.

A neatly grim example of this arose in July, when the Belgian parliament passed laws mandating the retention of user data by telecommunications and internet providers. This was a second run by the parliament, given the invalidation in April 2021 by the Belgian Constitutional Court of the previous data retention law. That particular statute permitted the storage of every Belgian's telecom, location and internet metadata for up to 12 months. Those behind the new law, such as the Minister of Justice Vincent Van Quickenborne, claim it to be a targeted measure that preserves privacy; in truth it permits general data surveillance.

In Germany, the debate has been particularly strident. In 2010, the Constitutional Court annulled the first data retention law. Five years later, data retention was re-introduced, though not implemented given court rulings.

Despite arguments favouring its implementation, the investigation and prosecution of crime could still take place with high degrees of success without any such regime in place. In January this year, the statistics on crime clearance rates published by the German

government revealed than a mere 3% of child sexual abuse material (CSAM) investigations between 2017 and 2021 could not be pursued for want of records of IP addresses.

The current coalition agreement, while supporting the retention of communications data, specifies that it be done "on an ad-hoc basis" and only via judicial order. But the Social Democratic Minister of the Interior, Nancy Faeser, is a steadfast devotee of such retention, a fan of indiscriminate surveillance.

Faeser and her surveillance fan club got an answer last month with the ruling by the Court of Justice of the European Union (CJEU) that Germany's general data retention law breached EU law. The case was triggered by action taken by Deutsche Telekom unit Telekom Deutschland and the internet service provider SpaceNet AG. The CJEU's opinion was duly sought by the German court. The judges duly found that "EU law precludes the general and indiscriminate retention of traffic and location data, except in the case of a serious threat to national security."

The court took issue with the law's "broad set of traffic and location data" retention requirements to be kept over periods of 10 weeks and four weeks respectively. This could lead to "very precise conclusions to be drawn concerning the private lives of persons whose data are retained, such as habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them and, in particular, enable a profile of those persons to be established."

The CJEU did not do away with the idea of bulk data retention, merely noting a growing list of exceptions that states are bound to exploit. In the German case, specific contexts might involve a grave threat to national security. There would also have to be court oversight, discrimination in terms of targeting, and a specific period of time.

In another joined case, the CJEU found that financial market regulators cannot use EU laws to target insider dealing and market manipulation by forcing telecom providers to supply the personal data of suspect traders to the authorities. The French law in question, justified on the basis of fighting crime, permitted the retention of such traffic data for up to one year from the day of its recording.

National legislation requiring telecommunications operators "to retain generally and indiscriminately the traffic data of all users of means of electronic communication, with no differentiation in that regard or with no provision made for exceptions and without establishing the link required [...] between the data to be retained and the objective pursued" fell outside what was "strictly necessary and cannot be considered to be justified, in a democratic society".

While European judicial bodies with teeth rein in the way data retention is used, when and if it should even be permitted, countries such as Australia continue to show faith in the very idea. Last month's hack of the country's second largest telecoms company, Optus, was a reminder that unnecessary data retention measures are an incitement for unlawful access.

In 2015, when the Data Retention Bill was introduced, advocates and those in the telecommunications industry had reason to be worried. In testimony to the Parliamentary Joint Committee on Intelligence and Security, Telstra Director of Government Relations, James Shaw, noted that the telco's practice over peak times such as New Year's Eve was to

only retain some data for a few hours before being overwritten. This was markedly shorter than the Bill's proposed two-year retention period.

Telstra's Chief Information Security Officer Michael Burgess also issued a warning that such legislative requirements would embolden hackers. "We would have to put extra measures in place … to make sure that data was safe from those that should not have access to it."

Electronic Frontiers Australia Executive Office Jon Lawrence was even more trenchant in explaining to the Joint Committee that such data retention requirements were an "unnecessary and disproportionate invasion of privacy" and would "literally be a honeypot to organised crime, to any sort of person who can potentially access it".

Despite such warnings, the Joint Committee approved the bill, subject to a number of vague and ineffectual recommendations about security and appropriate data use. This has left those in Australia vulnerable to data loss and unprotected by the woefully inadequate *Privacy Act 1988* (Cth). But even the European example shows us that the forces of law and order remain attritive in their efforts to undermine rights and liberties via requirements for data storage. Even in the face of judicial rulings and precedents, the attempt to maintain mass surveillance through data retention regimes remains a burning, threatening issue.

*

Note to readers: Please click the share buttons above or below. Follow us on Instagram and Twitter and subscribe to our Telegram Channel. Feel free to repost and share widely Global Research articles.

Dr. Binoy Kampmark was a Commonwealth Scholar at Selwyn College, Cambridge. He currently lectures at RMIT University. He is a regular contributor to Global Research and Asia-Pacific Research. Email: bkampmark@gmail.com

Featured image is from TruePublica
