medConfidential short briefing on the Investigatory Powers (Amendment) Bill

The Investigatory Powers (Amendment) Bill (the Bill) amends the Investigatory Powers Act 2016 (the 2016 Act). Much of the Bill is out of scope of medConfidential's areas of interest.

Part 1 – Bulk Personal Datasets

According to the definition in Clause 199(1)(b) of the 2016 Act, *"the nature of the [Bulk Personal Data]set is such that the majority of the individuals are not, and are unlikely to become, of interest to the intelligence service in the exercise of its functions"*

Part 1 of this Bill seems to allow the Intelligence Agencies to harvest data from (semi-) public sources and buy data from commercial data brokers, by adding clauses into the existing Act.

1) Can Ministers explicitly confirm that the existing (health data) safeguards in s206 of the 2016 Act will apply to all new bulk personal datasets under this act? Will the extra scrutiny given to health records in each Annual Report of the Investigatory Powers Commissioner (e.g paragraph 4.13)apply to these new categories of Bulk Personal Dataset?

2) To what extent are these new BPD categories expected to cover new activities, and to what extent is it merely deregulating somewhat existing activities?

3) We assume that the Agencies will be able to buy any data that is for sale anywhere in the world, and derive inferences from those datasets, which does not seem to be against HMG policy on 'foreigners', but to what extent does this also cover British citizens? For worldwide internet services selling data on users? And to what extent is there any distinction at all?

4) In Russia you can buy almost any government records on anyone; in the US you can buy the device identifiers of women who visit abortion websites or clinics – is this the sort of data this clause is expected to cover? Are there any boundaries?
    a) Will each purchase be subject to the usual "Value for Money" tests of the Treasury?

5) Regarding 226(3)(c+d+e) Can the Government clarify what procedure will apply to data sets that are "stolen", such as the 2014 Sony Hack, or data held by "ransomware" groups, or unpublished datasets held by journalists such as the Snowden archive?[1] Will any of these come newly into scope of the Agencies as a result of this Bill?

6) If data on British citizens is stolen and leaked, 226(3)(d+e) suggests it would then be fair game for any use by the Agencies; is this *newly* the case, or *already the case*?

7) To what extent does the "reasonable expectation of privacy" extend to other BPDs? Is there defined meaning of "reasonable" in UK law?[2] Parliamentarians have their email hosted by Microsoft on Office365 – the special status of Members aside – should anyone else with their email identically hosted have an expectation that the Agencies will be able to bribe a copy of everything they send or retain as BPD? When does a BPD cross the definitional boundary and become communications data?

[1] We would hope journalistic organisations pick apart the Snowden example in their own briefings.
[2] We are now beyond medConfidential's understanding of relevant law.

Section 226 of the 2016 Act will be ridiculously complicated after amendment. It is likely that there will be a series of technical breaches of the law due to the similar but different (and differently different) categories of BPD.

Clause 20 – A reckless power grab by the Suella Braverman's Home Office

Suella Braverman's Home Office wants to veto security upgrades to apps used by your doctors to talk to each other. These powers by the Home Office will limit how you can be protected by software updates on the devices that keep us and our data safe.

"Notices" from the Home Office can be provide to "telecommunications services" (WhatsApp, Facebook Messenger (and all Facebook services), Apple iMessage (and all iPhone/Mac), Signal, etc) telling them they must apply to the HO for approval if they wish to improve their products in ways the HO dislikes.

8) Given the Home Office policy appears to encourage insecure and hackable devices, to what extent will the results of those security holes and hacks become Bulk Personal Datasets under earlier parts of the Bill?

This Government's Home Office doesn't care for the views of civil society, but "Big Business" doesn't come any larger than Apple, literally, and Apple is so concerned about the consultation on these powers that they went on the record.

Clause 20 interacts with the Online Safety Act.

If the recent Online Safety Act was designed to make Britain the safest place to be online, this clause is designed to make Britain the most dangerous place to use a device online, as the Home Office wishes to be able to block bug fixes and safety upgrades, the same upgrades needed by UK Ministers and officials. We all use the same iPhones or copies of Whatsapp and Signal. They're either secure for everyone, or insecure for everyone.

The Online Safety Act creates high barriers to entry for new apps in the UK, the Home Office is placing obligations on existing apps around upgrades, including security patches.

9) Is the Government trying to create a "for Ministers only" auto-deletion feature in Whatsapp?

The professional obligations placed on doctors and nurses is that the tools they choose to use to communicate must be safe, ie they must be encrypted. That allows the technology choices to evolve over time while the professional standards endure. The Home Office seems to believe that only it should decide what "secure" means.

medConfidential
13 November 2023
coordinator@medConfidential.org