Written evidence submitted by Ray Corrigan (IPB 30)

Submission to Investigatory Powers Bill Committee

My name is Ray Corrigan. I'm a Senior Lecturer in the Maths, Computing & Technology Faculty of The Open University, though I write to you in a personal capacity.

Summary

1. The Investigatory Powers Bill Public Committee is being required to analyse the long and complex Draft Investigatory Powers Bill in an unreasonably short timescale.
2. I will focus this submission on one issue – the disproportionate nature of bulk collection and retention of communications data proposed in the Bill

Bulk collection & retention of communications data: circles of suspicion

1. There is a fundamental misunderstanding at large in Westminster – the idea that collecting and retaining bulk personal data is acceptable as long as most of the data is only "seen" by computers and not human beings; and it will only be looked at by persons with the requisite authority with the aid of the Investigatory Powers Bill "filter" if it is considered necessary. This is a seriously flawed but widely accepted line that has been promoted by successive governments for some years.

2. The logical extension of such an argument is that we should place multiple sophisticated electronic audio, video and data acquisition recording devices in every corner of every inhabited or potentially inhabited space; thereby assembling data mountains capable of being mined to extract detailed digital dossiers on the intimate personal lives of the entire population. They won't be viewed by real people unless it becomes considered necessary.

3. Indeed with computers and tablets in many rooms in many homes, consumer health and fitness monitoring devices, interactive Barbie dolls, fridges, cars and the internet of things lining up every conceivable physical object or service to be tagged with internet connectivity, we may not be too far away from such a world already.[1]

4. In the past two years both the Court of Justice of the European Union[2] and the European Court of Human Rights[3] have repeatedly rejected bulk indiscriminate personal data collection, retention and dissemination as incompatible with international human rights obligations.

5. In Zakharov v Russia (2015) the European Court of Human Rights said authorisation for surveillance of phone communications "must clearly identify a specific person … or a single set of premises" and "that a system of secret surveillance … may undermine or even destroy democracy under the cloak of defending it".

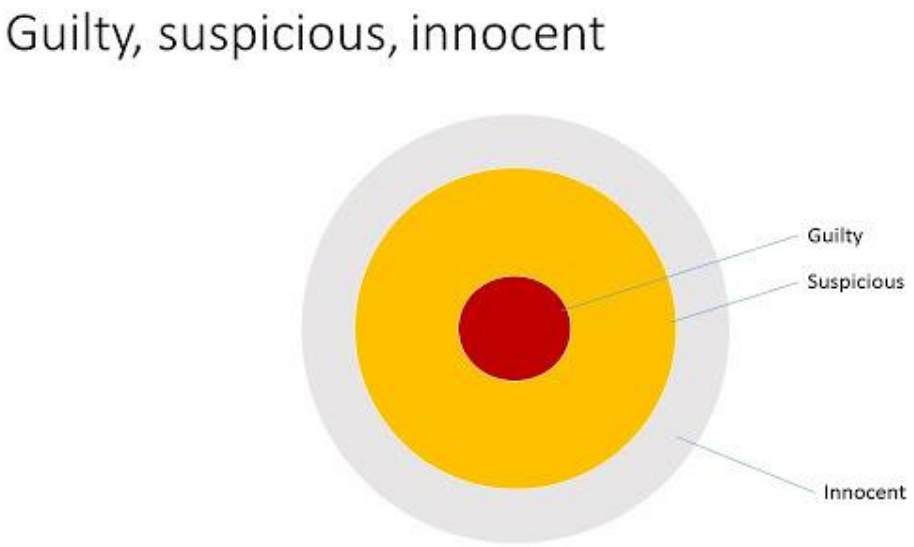
6. In Szabo & Vissy v Hungary (2016) the European Court of Human Rights ruled those authorising surveillance must "verify whether sufficient reasons for intercepting a specific individual's communications exist in each case."

7. Targeted not bulk surveillance is required.

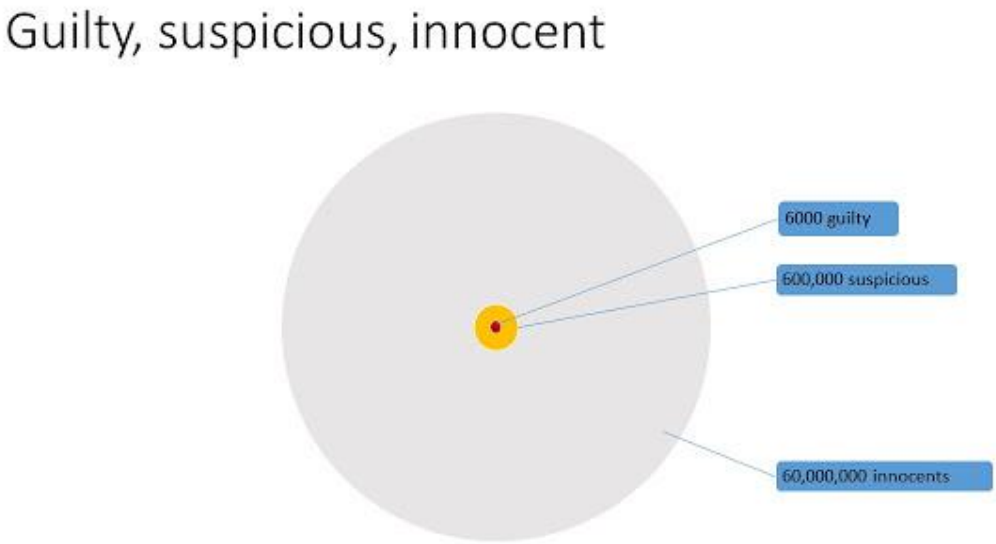
8. Leaving aside the legal situation, it is reasonable to suggest the guilty forfeit their right to privacy in connection with their nefarious activities. Authorities are entitled, also, to collect and peruse the data

[1] Executive Office of the President President's Council of Advisors on Science and Technology Report to the President, [May, 2014], Big Data and Privacy: A Technological Perspective
[2] Digital Rights Ireland (C-293/12 AND 594/12, 2014), Google Spain v Gonzales (C-131/12, 2014), Schrems (C-362/14, 2015)
[3] Zakharov v Russia (Application no. 47143/06, 2015), Szabo & Vissy v Hungary (Application no. 37138/14, 2016)

of the suspicious. Those in the suspicious category may be innocent but if law enforcement and the security services have a justifiable cause to harbour suspicion, they have a duty to investigate such persons. In the approach of the Investigatory Powers Bill the data of the innocent gets swept up in all this too. But that's not a problem, the government assures us, since law enforcement and the security services are not interested in the innocent.

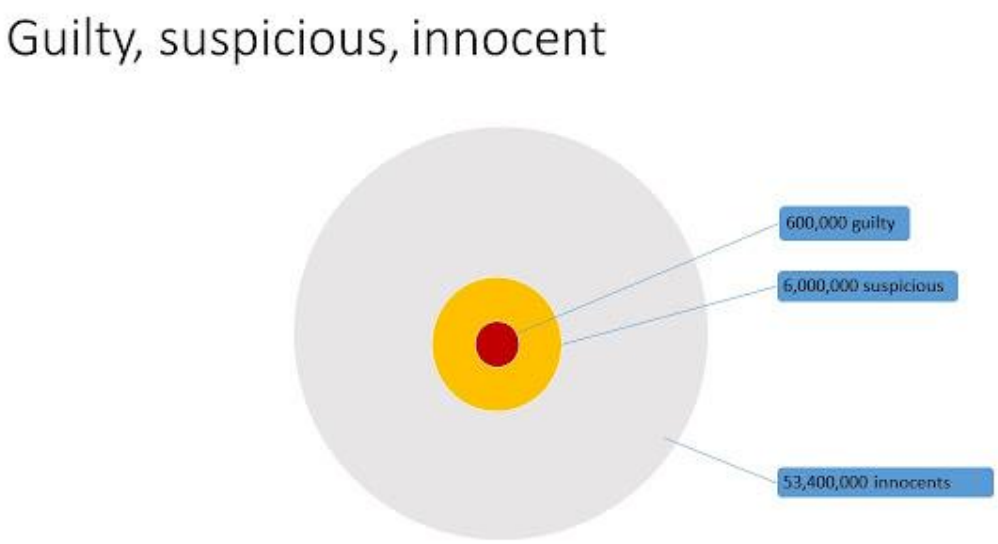


9. What do these circles of suspicion look like, however, if we consider relative proportions of guilty v suspicious v innocent by throwing some hypothetical numbers at the problem? Since successive government spokespersons for the past 16 years have talked in terms of thousands of dangerous individuals here, let's start with the hypothesis that there might be 6,000 dangerous people and 600,000 suspicious types resident in the UK, in a population of a little over 60 million. If that is anywhere close to the real numbers the relative areas of our guilty, suspicious and innocents' circles look like this (with the innocent circle drawn first and the suspicious and guilty circles thrown on top) –



10. So the collection – and/or the forced industry collection and retention for perusal by government authorities through the Investigatory Powers Bill "filter" – of everyone's data, in bulk, for investigatory

purposes, begins to look somewhat disproportionate. And it is not just industry that may be obliged to collect this data. Data retention and other powers demands may even be visited upon those running private and home networks. (And equipment interference warrants - targeted, thematic and bulk – may also be targeted at private/home networks but that's a whole other discussion which I'd recommend talking to Graham Smith, partner at Bird & Bird LLP, about). If the numbers of guilty rise to 600,000 and the suspicious to 6 million the picture changes again -



11. By playing around with the relative numbers we can get a picture of how big we think the guilty and suspicious circles have to get, before we consider it proportionate to justify the bulk data collection and retention powers in the Investigatory Powers Bill.

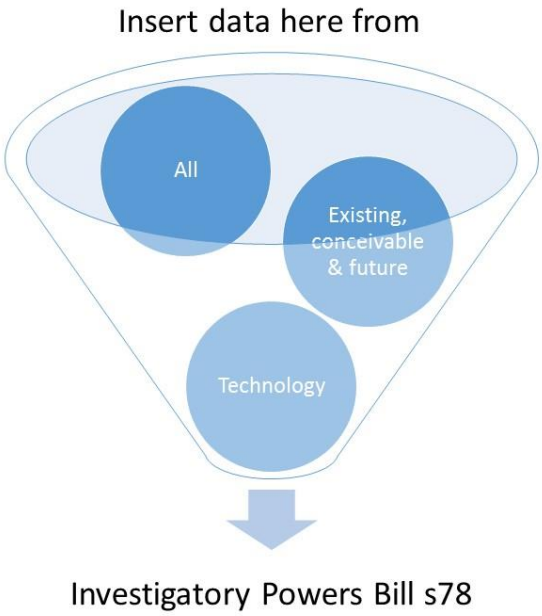
12. Even in that third scenario where it was assumed there were 600,000 guilty and 6 million suspicious, it doesn't look reasonable that the remaining 54 million or so innocents get dragged into the digital net of suspicion.

13. The bottom line is that we only start to get a real picture of what the Investigatory Powers Bill bulk data collection and retention powers mean when we get into the detail of how they will operate or are expected to operate in practice.

14. Internet connection records (ICRs) are one specific area of interest here, though it is still not clear, from the Bill or government explanations or associated documents, what exactly ICRs will be in practice. Government, or industry and others on government's behalf, should not be collecting, indiscriminately, for perusal and analysis, primarily electronic or otherwise, the reading, viewing and listening lists and other online activities of the entire population. Especially not those of tens of millions of innocents. It constitutes an unnecessary and disproportionate abuse of power.

15. I will conclude by drawing your attention to clause 78 of the latest version of the Bill, in which "relevant communications data" appears to be a catch all to cover the collection of just about any data. May I commend to you Graham Smith's pictorial representation of what this appears to mean available with an informative commentary at http://cyberleagle.blogspot.co.uk/2016/03/relevant-communications-data-revisited.html

16. As an engineer, s78 looks, to me, like this –



17. Indiscriminate bulk personal data collection and retention should be removed in all its forms from the Bill.

March 2016