The implications of ‘bulk hacking’

26/07/2019

Corporate Crime analysis: Matthew Richardson, barrister at Henderson Chambers, examines the concept of ‘bulk hacking’ by intelligence services and some of the legal implications, in light of the latest judicial review challenge by Liberty.

What is ‘bulk hacking’ and what is the context and background of it being used by GCHQ and other government agencies?

Bulk hacking is the colloquial name for the wide ranging powers given under the Investigatory Powers Act 2016 (IPA 2016) to the security and intelligence services, police forces and various government agencies allowing them to intercept or obtain, process, retain and examine private information of very large numbers of people—in some cases, the whole population. This includes the serious invasion of journalistic and watchdog organisations’ materials, lawyer–client communications and other privileged communications.

Liberty is challenging, under the Human Rights Act 1998 (HRA 1998), by way of judicial review the compatibility of IPA 2016 with HRA 1998, art 8 (right to a private and family life) and art 10 (right to freedom of expression). The case is *R (on the application of Liberty) v Secretary of State for the Home Department and Secretary of State for Foreign and Commonwealth Affairs*, case no CO/1052/2017 in the High Court, QBD.

The National Union of Journalists (NUJ) has joined the claim in support of Liberty’s position, particularly emphasising the freedom of expression elements of the argument and the effect on journalists.

This claim follows on from another similar claim brought by the privacy rights group, Big Brother Watch, on the back of Edward Snowden’s revelations, and resulted in the government conceding that the oversight regime for such data gathering and processing was insufficient and may need to be changed.

Does IPA 2016 allow for bulk hacking and why? What are the arguments in favour of bulk hacking? Are there any restrictions in place under IPA 2016?

IPA 2016 does allow for bulk hacking. It gives authorisation for what it calls ‘equipment interference’ or what the average person would think of as computer hacking in IPA 2016, parts 5 and 6, bulk data retention and processing in IPA 2016, pt 7, bulk interception of communications, including mobile phones in IPA 2016, pt 6, and most interesting bulk acquisition of and retention of communications data, which requires, for example, mobile phone providers to hand over vast amounts of metadata associated with the use of their networks, from all users, even if they are not even suspected of a crime, in IPA 2016, parts 3, 4 and 6.

The ministers defending the judicial review contend that the powers under challenge are of critical importance to, and are effective in securing, the protection of the public from a range of serious and sophisticated threats arising in the context of terrorism, hostile state activity and serious and organised crime.

There are several restrictions in place under IPA 2016 including most crucially its oversight by the Investigatory Powers Commissioner, currently the very highly regarded Lord Justice Fulford, who is assisted by 15 commissioners who are senior members of the judiciary and a large staff including a number of technical experts.

However, it is Liberty’s case that the current regime has insufficient safeguards in a democratic society.

Why has bulk hacking been criticised and what legal/human rights issues does it pose? Are there any potential cyber risks?

Bulk hacking has been criticised for number of relatively obvious reasons which include that, as with any dragnet style data gathering exercise, a number of completely innocent law abiding citizens may find their computers hacked, their

data gathered and processed, their mobile phone intercepted, and their most private and confidential information trawled through by the government, including legally privileged lawyer/client communications.

The NUJ argues that this type of surveillance can be used to the detriment of free journalism and will almost certainly have a chilling effect on the kind of journalism that should be allowed to exist unencumbered in an advanced democratic society.

There are potentially cyber risks associated with this, too. Bulk hacking may, as a natural by-product of its successful deployment, leave systems vulnerable to hacks from other malicious, non-governmental actors.

There is also a non-zero risk that personal data of law abiding citizens will be processed in a manner that may cause them substantial distress and result in unnecessary interference in their private lives.

What will happen if the government loses this case and what will be the legal implications?

The first and most visible consequence for the government will be a huge political embarrassment. The fact that the government could produce a workable scheme for bulk surveillance even after a number of steers from the European Courts will not bode well for the new Prime Minister.

Secondly, it will open the door to damages claims, from individuals who have been adversely affected by the incompatible regime, given the large numbers involved, a group action could be very costly for the government indeed.

Finally, the government will have to go back to the drawing board, and try to find a regime for wide scale surveillance that will satisfy the courts, keep the people of the United Kingdom safe and maintain our obligations with our overseas intelligence partners—no easy task.

Interviewed by Alex Heshmaty.

The views expressed by our Legal Analysis interviewees are not necessarily those of the proprietor.