Chambers of Lawrence Power
4 King's Bench Walk,
Temple, London, EC4Y 7DL
Tel: 02078228822 Fax: 02078228844

*This article was first published on Lexis®PSL Corporate Crime on 20 August 2019. Click for a free trial of Lexis®PSL.*

# Lawfulness of bulk hacking powers under the Investigatory Powers Act 2016 (R (Liberty) v Secretary of State for the Home Department)

20/08/2019

**Corporate Crime analysis: Adam Richardson, barrister at Whitestone Chambers, considers the most recent judicial review challenge brought by Liberty concerning the lawfulness of the bulk hacking powers under the Investigatory Powers Act 2016 (IPA 2016).**
*R (on the application of National Council for Civil Liberties (Liberty)) v Secretary of State for the Home Department and another (National Union of Journalists intervening)* [2019] EWHC 2057 (Admin), [2019] All ER (D) 02 (Aug)

## What are the practical implications of this case?

As the claimants effectively lost the case, the existing regime vis-a-vis IPA 2016 still stands—arguably even more firmly than before. As such, there will be no new practical implications to consider other than those already created by IPA 2016. The largest concern for lawyers has to be the effect on legal professional privilege (LPP). Ever since the Regulation of Investigatory Powers Act 2000 (RIPA 2000), there has been a question of a surveillance authority legally acquiring information that is the subject of LPP. This goes against years of convention protecting privilege, however RIPA 2000 remained silent on the topic. When IPA 2016 was first drafted, the Bar Council raised explicit concerns about the erosion of LPP through either a failure to distinguish between privileged and non-privileged communications (as a result of bulk hacking) or the power given to authorities to monitor 'sensitive, highly confidential communications that have nothing to with criminality, national security or threats to individuals'.

The government listened and added a few additional safeguards for privileged information. A warrant would be required to be issued for the interception and review of information that is subject to LPP. The authority issuing the warrant must have regard to the 'public interest in the confidentiality of items that are subject to legal privilege'. Further, IPA 2016 also requires public interest, necessity and prevention of death, or serious injury conditions to be satisfied before such a warrant can be issued. Needless to say, this is a very high bar. There can be no getting around that as a result of bulk hacking, privileged information will be intercepted if only through inadvertence. Given the number of practical and operational issues raised by the claimant in the case, this should be concerning at best. The claimants have made clear they intend to appeal this, and it may end up in the European Court of Human Rights (ECtHR) where there may well be a different view taken, so, until all appeals are exhausted on this matter, no position is settled.

## What was the background?

The High Court's judgment in *Liberty, R (On the Application Of) v Secretary of State for the Home Department & Another* is the second iteration of the issues raised on this claim. See *R (on the application of the National Council for Civil Liberties (Liberty)) v Secretary of State for the Home Department and another* [2018] EWHC 975 (Admin), [2018] 3 WLR 1435, , [2018] All ER (D) 129 (Apr), where the court gave judgment on the first part of the claimant's challenge to IPA 2016. That challenge was brought under EU law. It only concerned IPA 2016, Pt 4 (regarding powers to require the retention of 'communications data'), as this part had just been brought into force. The court found

in that judgment that IPA 2016, Pt 4 was incompatible with human rights law and gave the government until 1 November 2018 to redraft it, which it duly did.

In the instant judgment, the court was concerned with the second part of the claimant's challenge, which arises under the Human Rights Act 1998 (HRA 1998). This challenge concerns various other parts of IPA 2016, which have now been brought into force on various dates.

The claimant challenged four different sets of provisions in IPA 2016. What they all have in common is that they concern bulk powers, rather than powers which are directed at any particular individual who may be a potential subject of interest (sometimes called targeted surveillance). The relevant provisions are as follows:

• IPA 2016, Pt 6, Ch 1—which relates to bulk interception warrants

• IPA 2016, Pt 6, Ch 3, and IPA 2016, Pt 5—these concern warrants for bulk and thematic equipment interference. The claimant has described this in its submissions as 'hacking'

• IPA 2016, Pt 7, which relates to warrants for bulk personal datasets (BPD)

• IPA 2016, Pt 6, Ch 2, and IPA 2016, Pt 3–4—respectively warrants for bulk acquisition of communications data and retention notices for, and acquisition of, communications data. Communications data is not the content of communications but other matters such as where, when and who

The only remedy which the claimant sought was a declaration of incompatibility under HRA 1998, s 4.

A very simplistic summary of the claimant's case is that the minimum safeguards established by the ECHR for secret surveillance regime were not met. As not all human rights are absolute, certain breaches may only take place where they are in accordance with law or necessary for a democratic society. The claimant submitted the measures in IPA 2016 were neither necessary nor proportionate.

**What did the court decide?**

The court went to great pains in this judgment to be as comprehensive as possible. The judgment itself is almost 400 paragraphs long (excluding accompanying legislation) and gives an incredibly detailed overview of the law. While the claimant was able to bring to light shocking examples of government data use, including data being lost in ungoverned spaces without the necessary controls, among others, the court still found that IPA 2016 was not incompatible with HRA 1998. Among the extensive reasoning is that the mechanisms for oversight within the legislation itself, such as the establishment of the office of the Investigatory Powers Commissioner (to conduct independent oversight of spy agencies' use of the powers), provide sufficient checks on the risk of abuse. The court dubbed the regime as 'a suite of interlocking safeguards'.

The court spoke specifically of Parliament's consideration for the fears about abuse expressed by the claimant but noted they chose to address those in IPA 2016 through those various interlocking safeguards mentioned.

*Interviewed by Alex Heshmaty.*