Department for Digital, Culture, Media & Sport

Margot James MP
Minister for Digital and the Creative Industries
4th Floor
100 Parliament Street
London SW1A 2BQ

www.gov.uk/dcms
enquiries@culture.gov.uk

Sir William Cash MP
Chair of the European Scrutiny Committee
House of Commons
London
SW1A 0AA

TO2018/16528/DC
20 December 2018

Dear Bill

Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)

Further to my letter of 18 June, I am writing to provide an update on the proposed EU ePrivacy Regulation (5358/17) and to address the questions from the Committee's 21 March report.

Discussions in Council have been ongoing since my last update. As the Austrian Presidency's progress report set out, and as shown by the discussion at the 4 December Telecoms Council, there continues to be debate on the most complex articles of the proposed Regulation text (Articles 6, 8 and 10). Member States have also continued to seek clarity on two principal issues: the relationship between the proposed Regulation and the GDPR, and which services will be captured by the scope of the Regulation. For the above reasons, many Member States are yet to take a position on the text until this is clarified.

As you are aware, the Government takes both the protection of personal data and the right to privacy extremely seriously and we welcome the opportunity to update the current ePrivacy Directive, to address technological developments and the evolving digital landscape. We reached collective agreement on the UK's negotiating position on the Regulation on 29 November. We believe that the Austrian Presidency's Council text is going in the right direction, however we still have a number of concerns with some articles in the proposed Regulation, which, if we do not get right could: lead to legal uncertainty for those who have to apply the Regulation; restrict some legitimate and proportionate data processing from taking place; and may impact digital innovation.

Specifically, we believe that the legal bases for processing should align further with the legal bases from the GDPR. A more risk-based approach is necessary to ensure that legitimate reasons for processing data, such as in instances of vital interests, are not negatively impacted. There should be proportionate flexibility for stakeholders to perform their functions and for future technological developments, whilst at the same time ensuring that robust data protection and privacy standards are in place.

We also believe that the text needs to be clear that processing electronic communications data for the purposes of tackling crimes such as online child sexual exploitation is not restricted (or that it is sufficiently covered in other legislation). We appreciate the Austrian Presidency's attempt to clarify this issue through specifying in the text (Recital 26) that processing electronic communications for the '*prevention, investigation, detection or prosecution of criminal offences, including dissemination of child pornography*' can be exempted by Member State law, however the requirement for individual Member State action is likely to make the exemption ineffective given:

- sharing imagery or victim to offender communications commonly involve individuals in different countries or jurisdictions communicating with each other;
- data may be stored in multiple or indeterminate jurisdictions rendering the risk to service providers of being in breach too high;
- There is a high risk that existing scanning may not be continued if service providers are not certain that an adequate exemption for this has been enacted in all Member States.
-

We believe that an explicit condition permitting this processing under Article 6 is vitally important. This is a global issue, which requires a coordinated multilateral approach to tackling it.

Encryption

The Committee enquired about the UK's position on the (then) proposed Article 17 of the ePrivacy Regulation. This Article has now been removed from the draft ePrivacy Regulation text and was replicated in Article 40(3) of the recently recast European Electronic Communications Code (EECC). The scope of Article 40(3) targets network and service operators; Over The Top Providers (OTTs) would not come under its scope as they do not control signal conveyance across the network. In the EECC negotiations there was consensus across the majority of Member States to explicitly remove proposed mandatory encryption requirements.

The UK does not support the mandating of end-to-end encryption. The Government is in favour of strong encryption: it is critical to protect UK citizens from harm online and billions of people worldwide use it every day for a range of services including banking, commerce and communications. But, like many powerful technologies, encrypted services are abused by a small minority of people. There is a particular problem with end-to-end encryption where certain providers have deliberately designed their systems so that even they cannot see the content of the message, preventing them from complying with lawful requests for exceptional access.

The abuse of end-to-end encryption by terrorists and other criminals is having a significant impact on the ability of UK agencies responsible for national security and serious criminal investigations to access the content of lawfully intercepted messages. We do not want unfettered access to all communications but we do need to ensure our law enforcement and intelligence agencies are able to gain lawful and exceptional access to the communications they need to keep us safe. We want to work with service providers to fulfil our collective responsibility to protect us from terrorists and those who commit serious crimes, while allowing providers to protect user privacy. The actual solutions that can deliver the access to the information we require will depend on the technology, architecture and functionality of each provider's systems. We believe there are potential technical options that could deliver exceptional access to the

communications of terrorists and criminals without undermining the privacy of lawful users.

National Security

The Committee also enquired about the impact of the proposed ePrivacy Regulation on national security activities. The ePrivacy Regulation is intended to repeal and replace the current ePrivacy Directive (Directive 2002/58/EC) which was the EU legislation considered by the Court of Justice of the European Union (CJEU) in the Watson/Tele 2 judgment (C-698/15 and C-203/15). The Investigatory Powers Tribunal (IPT) has made a reference to the CJEU asking whether that judgment applies to bulk communications data acquired from telecommunications operators by the intelligence agencies and, if so, to what extent (in the Privacy International case which is listed as C-623/17 before the CJEU). The IPT expressed its concern about the impact of the Watson/Tele 2 judgment to such retention and access, and the Government agrees. The Government's position is that the judgment does not apply and it is defending this before the CJEU. We expect the case will be heard in the CJEU next year with a judgment following roughly six months later.

Since April 2017, Member States have collectively been considering the impact of the judgment in the context of the ePrivacy Regulation proposal. Consistent with the Government's position in the IPT reference, it is seeking to ensure that the provisions of the proposed Regulation, should it be adopted, do not impact on national security activities. We believe that the text needs to be clear that national security is outside the scope of Union law. The UK is not alone in looking at the boundaries of the decision in Watson/Tele2, including whether it applies to national security activities. Further references have been made to the CJEU by courts in Belgium (C-520/18) and France (C-511/18 and C-512/18). Those cases are proceeding behind the Privacy International case.

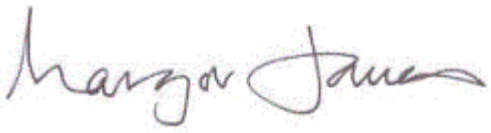
Applicability

The Committee also asked about the implications of the Regulation either being adopted during the implementation period or adopted after the implementation period. The proposed Regulation is yet to be agreed and timing of applicability is uncertain. We will continue to work with other Member States in Council to ensure that the proposals protect the confidentiality of electronic communications while encouraging digital innovation. Under the provisions on the implementation period in the Withdrawal Agreement, Union law on the protection of personal data, including the current ePrivacy Directive and any other Union law which becomes applicable during the implementation period, will continue to apply to personal data during the implementation period.

The current Council text has proposed a 24 month transposition period before the Regulation would become applicable (after it has been adopted), the original Commission proposals sought for the Regulation to become applicable at the same time as the GDPR, but that was unattainable. The proposed ePrivacy Regulation will apply automatically in the UK if it becomes applicable in the EU before the end of the implementation period. The UK will take an active diplomatic interest in any measures which will affect the UK during the implementation period as part of our dialogue with the Institutions and Member States. If the Regulation is adopted and becomes applicable after the implementation period, we would need to consider whether there would be any advantage in updating our domestic law to reflect the Regulation. We will continue to ensure that our domestic legislation has high standards on protecting personal data and the right to privacy, as well as encouraging innovation in the data economy.

I am copying this letter to Lord Boswell of Aynho, Chair of the European Union Committee; Rt Hon Norman Lamb, Chair of the Science and Technology Committee, Les Saunders, DExEU; and James Ainsworth and Rachel Marnick, DCMS.

Yours ever



MARGOT JAMES MP
Minister for Digital and the Creative Industries