PRIVACY INTERNATIONAL'S RESPONSE TO THE UK GOVERNMENT CONSULTATION ON REVISED NOTICES REGIMES IN THE INVESTIGATORY POWERS ACT 2016

I. INTRODUCTION

Privacy International (PI) appreciates the opportunity to respond to the Government's consultation on the proposed outcomes for amended regimes for technical capability notices, data retention notices and national security notices. PI is a London-based non-profit, non-governmental organisation (Charity Number: 1147471) that researches and advocates globally against government and corporate abuses of data and technology. It exposes harm and abuses, mobilises allies globally, campaigns with the public for solutions, and pressures companies and governments to change. PI challenges overreaching state and corporate surveillance so that people everywhere can have greater security and freedom through greater personal privacy. Within its range of activities, PI investigates how peoples' personal data is generated and exploited, and how it can be protected through legal and technological frameworks. It has advised and reported to international organisations like the Council of Europe, the European Parliament, the Organisation for Economic Cooperation and Development, the UN Office of the High Commissioner for Human Rights, and the UN Refugee Agency.

PI remains concerned about the existing powers in the Investigatory Powers Act and will continue to challenge them until they are necessary and proportionate. We have worked in dozens of countries across the world and have followed technology policy debates in countless jurisdictions. The UK Government already possesses globally unprecedented powers, some of which should not exist in a democratic society, and those that are within reason are lacking adequate human rights safeguards. With our experiences closely tracking the progress of the Act (and before that, RIPA 2000), we are well versed in how little the Home Office respects privacy safeguards in law and practice. Consequently, we are disappointed by the narrow focus of the present call and we invite the Government to open the Act and all surveillance powers, whether written in law or assumed, for a broader review, as had occurred in the 2006-2009 period after prior years of excess. Considering our substantial UK litigation experience in the last decade, much needs repairing in UK surveillance policy.

For more than 10 years, PI has focused sustained attention on the issue of government surveillance, by carrying out extensive legal and policy work. We have brought several challenges, before UK courts[1] as well as the European Court of Human Rights,[2] against the UK government's surveillance powers. Most recently and following a challenge brought by PI and Liberty, the Investigatory Powers Tribunal (IPT) found that there were "very serious failings" at the highest levels of MI5 to comply with privacy safeguards from as early as 2014, and that successive Home Secretaries did not enquire into or resolve these long-standing rule-breaking despite obvious red flags.[3] In addition, we were heavily involved in

[1] See, for example, R (on the application of Privacy International) v Investigatory Powers Tribunal, [2019] UKSC 22; Privacy International v Investigatory Powers Tribunal, [2021] EWHC 27 (Admin); Privacy International v Secretary of State for Foreign and Commonwealth Affairs and others, [2021] UKIPTrib IPT_15_110_CH.
[2] See, for example, 10 Human Rights Organisations v. United Kingdom, App.No. 24960/15, 25 May 2021 [GC]; Privacy International and Others v. United Kingdom, App.No. 46259/16, 3 September 2020 (decision).
[3] Liberty and Privacy International v the Security Service and Secretary of State for the Home Department, [2023] UKIPTrib IPT/20/01/CH. See also, PI, Press: Landmark ruling exposes years of rule breaking by MI5 (30 January 2023), https://privacyinternational.org/press-release/5027/press-landmark-ruling-exposes-years-rule-breaking-mi5.

the debate surrounding the passing of the Investigatory Powers Act (IPA) 2016 and gave written and oral evidence before the relevant parliamentary Committees.[4]

Without prejudice to whether there is an actual necessity for the existence or use of potentially extremely intrusive - and at times unchecked - surveillance powers, such as those prescribed under the IPA 2016, the present submission comprises PI's comments on the five overarching objectives that were put forward by the Government on 5 June 2023.[5] Our comments focus on the equipment interference powers that may be contained in a National Security Notice (NSN) or a Technical Capability Notice (TCN) served by the Secretary of State to a telecommunications operator.

The present submission is structured as follows: first, we briefly outline the security and privacy issues surrounding the current IPA regime regarding National Security Notices and Technical Capability Notices ordering operators to conduct equipment interference. Second, we provide our specific comments on each of the proposed objectives. Finally, we discuss the implications the proposed changes would have for the current and future adequacy decisions enabling data transfers between the UK and the EU.

II. PRIVACY AND SECURITY ISSUES SURROUNDING NSNs AND TCNs REQUIRING OPERATORS TO CARRY OUT CONDUCT THAT AMOUNTS TO EQUIPMENT INTERFERENCE

Under the IPA 2016, both NSNs and TCNs served by the Secretary of State to telecommunications operators may require them to, among others, carry out activities that would facilitate intrusive forms of surveillance such as interception and equipment interference.[6] For example, Section 252(3) IPA 2016 stipulates that an NSN may require an operator to facilitate "*anything done by an intelligence service under any enactment other than*" the IPA 2016 (such as the Intelligence Services Act 1994, which has been used to authorise non-investigative forms of equipment interference) or "*to provide services or facilities for the purpose of assisting an intelligence service to carry out its functions more securely or more effectively*", while Section 253(5) IPA 2016 states that a TCN may, among others, include obligations relating to equipment owned by an operator, obligations "*relating to the removal by a relevant operator of electronic protection applied by or on behalf of that operator to any communications or data*" or obligations relating to the security of the services provided by an operator.

The privacy and security implications of NSNs and TCNs are potentially profound. Their impact could be even more significant than the targeted or bulk warrants authorised under other parts of the IPA 2016 because NSNs and TCNs can require systemic change. That is, using a TCN or NSN, the Government can demand that operators alter their services in a way that may affect all users. For instance, a TCN requiring the "*removal by a relevant operator of electronic protection*" could be used

[4] PI, Privacy International Submission in Response to Science & Technology Committee Call for Evidence on the Draft Investigatory Powers Bill (27 November 2015), https://privacyinternational.org/sites/default/files/2017-12/PrivacyInternational_ScienceTechSubmission.pdf; Privacy International & Open Rights Group, Submission to the Joint Committee on Human Rights on the Draft Investigatory Powers Bill (7 December 2015), http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/human-rights-committee/legislative-scrutiny-draft-investigatory-powers-bill/written/25654.pdf; Joint Committee on the Draft Investigatory Powers Bill, Internet service providers and civil liberties groups give evidence (9 December 2015), https://www.parliament.uk/external/committees/joint-select/draft-investigatory-powers-bill/news/2015/civil-liberties-internet-providers-evidence; PI, Submission to the Joint Committee on the Draft Investigatory Powers Bill (21 December 2015), https://privacyinternational.org/sites/default/files/2017-12/Submission_IPB_Joint_Committee.pdf.

[5] UK Home Office, Consultation on revised notices regimes in the Investigatory Powers Act 2016 (5 June 2023), https://www.gov.uk/government/consultations/revised-investigatory-powers-act-notices-regimes-consultation/consultation-on-revised-notices-regimes-in-the-investigatory-powers-act-2016-accessible-version.

[6] In the present submission, the terms Equipment Interference (EI) and Computer Network Exploitation (CNE) are used interchangeably.

to force a service such as WhatsApp or Apple to remove or undermine the end-to-end encryption of the services it provides worldwide.[7] End-to-end encryption is very important for preserving the privacy and security of messages,[8] as noted, inter alia, by UN resolutions of the General Assembly and the Human Rights Council.[9] Similar powers currently being considered under the Online Safety Bill have prompted a number of companies to publicly announce they would resist complying and might leave the UK market if such a demand were made.[10] Given that some of the companies which could be targeted by TCNs and NSNs provide systems used by millions or billions of people, the impact of a forced change to such systems would be incredibly far reaching.

TCNs or NSNs might also be used to force a company to send false security updates to its users, or to refrain from fixing a vulnerability in its systems, both of which could be used to facilitate equipment interference. Equipment interference pertains to the exploitation of computer networks. This intrusive surveillance technique has the potential to undermine the security of targeted devices, networks or infrastructure, and potentially even the internet as a whole.[11] This is because the relationship between users and companies is based primarily on trust. People's trust in the devices, networks, and services is constantly threatened by unintended errors or bugs. These bugs may give rise to vulnerabilities and be exploited by third parties. It is a constant struggle for software developers and testers to discover and fix these bugs before they are used for malicious purposes. Equipment interference often depends on exploiting vulnerabilities in systems to facilitate a surveillance objective. It may also involve manipulating people to interfere with their own systems, such as could be accomplished by a false security update. These techniques prey on user trust, the loss of which can undermine the security of systems and the internet.[12]

It should be recalled that Article 8 of the European Convention on Human Rights "*may also impose on the State certain positive obligations to ensure effective respect for the rights protected*" by it.[13] While the European Court of Human Rights has recognised that states enjoy a certain margin of appreciation in choosing how to realise the protections enshrined in Article 8, their discretion is not unlimited, especially in a field such as communications surveillance where the potential for abuse is extremely high.[14]

At the same time, such blanket or indiscriminate measures that seriously interfere with privacy are neither necessary nor proportionate. In *S. and Marper*, the Grand Chamber of the European Court of Human Rights held unanimously that the collection and retention of DNA and fingerprints of innocent people was contrary to Article 8.[15] In particular, the Court was "*struck by the blanket and indiscriminate nature of the power of retention in England and Wales*",[16] concluding that "*the blanket and indiscriminate nature of the powers of retention…fails to strike a fair balance between the*

[7] Section 253(5)(c) IPA 2016.
[8] See, See PI, Securing Privacy: PI on End-to-End Encryption, https://privacyinternational.org/report/4949/securing-privacy-end-end-encryption.
[9] See recently, A/RES/77/211 and A/HRC/RES/48/4.
[10] Mary-Ann Russon, Online Safety Bill: WhatsApp, Signal issue stark final warning against mass snooping of messages (4 July 2023), https://www.standard.co.uk/tech/online-safety-bill-whatsapp-signal-element-breaking-encryption-mass-surveillance-messaging-apps-b1091873.html.
[11] PI, Government Hacking, https://privacyinternational.org/learn/government-hacking.
[12] PI, Will They Hack Us? Will They Betray Us? (24 November 2015), https://privacyinternational.org/news-analysis/1337/will-they-hack-us-will-they-betray-us.
[13] See, *inter alia*, X and Y v. the Netherlands, App. No. 8978/80, para 23; Von Hannover (no. 2) v. Germany, App. Nos. 40660/08 60641/08, para 98; Hämäläinen v. Finland, App. No. 37359/09, para 62.
[14] See, Klass and Others v. Germany, App. No. 5029/71, para 50; Roman Zakharov v. Russia, App. No. 47143/06, paras 232-234.
[15] S. and Marper v. the United Kingdom, App.Nos. 30562/04 and 30566/04, 4 December 2008 [GC].
[16] Ibid, para 119.

competing public and private interests".[17] It held that the UK had "*overstepped any acceptable margin of appreciation in this regard*" even though the DNA database was undoubtedly a valuable tool for detecting and prosecuting serious criminals.

While the IPA 2016 provides some safeguards, by, for instance, requiring the Secretary of State to ensure that certain requirements are met before issuing a notice under Sections 252(1) and 253(1), and that a "*decision to give the notice has been approved by a Judicial Commissioner*",[18] its provisions still raise concerns about their compatibility with international human rights law standards, including those enshrined in the European Convention on Human Rights (ECHR).[19] The European Court of Human Rights has applied a heightened standard of 'strict necessity' to interferences with the right to privacy when using "cutting-edge" technologies in a secret surveillance context.[20] Similarly, the UN High Commissioner for Human Rights has highlighted the privacy risks posed by measures that undermine encryption of communications and security of devices through government hacking and he recommended that governments "*avoid all direct, or indirect, general and indiscriminate restrictions on the use of encryption, such as prohibitions, criminalization, the imposition of weak encryption standards or requirements for mandatory general client-side scanning; interference with the encryption of private communications of individuals should only be carried out when authorized by an independent judiciary body and on a case-by-case basis, targeting individuals if strictly necessary for the investigation of serious crimes or the prevention of serious crimes or serious threats to public safety or national security*".[21]

As explained below, should the Government's proposed Objectives, which essentially seek to deprive an already faulty surveillance regime of indispensable safeguards, make it into law, the UK would not only be failing to live up to its human rights law obligations, but it would be also jeopardising the privacy and security of every Internet user in the world.

III. COMMENTS ON THE PROPOSED OBJECTIVES

OBJECTIVE 1

Objective 1 seeks to impose a general requirement for operators to comply with the potential requirements of a notice during the review period and before the latter is formally served, allowing the Home Office to maintain access to any data sought through the notice served. This proposal is extremely concerning as it appears to be an end run around the already insufficient safeguards for issuing NSNs and TCNs.

Such a change to the notice regime would allow the Government to force telecommunications operators to comply with any orders to maintain the status quo given by the Secretary of State without those orders having been reviewed by a Judicial Commissioner or incorporated into a formal notice. At the same time, a review process could potentially last indefinitely without necessarily resulting in a formal notice being served to the relevant operator. During that review process the operator would be left without any clear remedies to object or challenge the review. The same is to be noted about

[17] Ibid, para 125.
[18] See, Section 252(1)(c) and Section 253(1)(c) IPA 2016.
[19] For a detailed overview of the current international human rights law standards and surveillance see, PI, PI's Guide to International Law and Surveillance (Version 3.0, December 2021), https://privacyinternational.org/sites/default/files/2022-01/2021 GILS version 3.0_0.pdf.
[20] Szabó and Vissy v Hungary, App No 37138/14, ECtHR, § 73 (12 January 2016); see also, Liblik and Others v Estonia, App Nos 173/15 and 5 others, ECtHR, § 131 (28 May 2019) ("*powers to instruct secret surveillance of citizens are only tolerated under Article 8 to the extent that they are strictly necessary for safeguarding democratic institutions*").
[21] Report of the UN High Commissioner for Human Rights on the right to privacy in the digital age, 04 August 2022, UN Doc A/HRC/51/17, para 57(b).

review processes that do not result in a formal notice being served. In those cases, the review process of the notice regime could easily be abused by serving as a mechanism for the Secretary of State to stop relevant operators from using specific forms of technology or to obtain access to data with regard to controversial topics which would, under the current IPA regime, fail to obtain the necessary approval by the Judicial Commissioner or survive a legal challenge brought by an operator. For example, instead of subjecting it to a transparent and democratic debate, which might accordingly trigger strong public and corporate opposition,[22] the Government could now pursue its recurring ambition to circumvent end-to-end encryption,[23] by engaging in a never-ending review process with operators, who will have little choice but to comply with any unchecked demands imposed upon them and who eventually might never be served with a formal notice.

Hence, Objective 1 raises major compatibility issues with Articles 8 and 13 of the European Convention on Human Rights as it enables mass or intrusive surveillance in absence of any prior independent authorisation. The importance of prior independent authorisation of surveillance measures has been repeatedly emphasised by the European Court of Human Rights[24] as well as other international bodies.[25] In *Szabo and Vissy v. Hungary*, the European Court of Human Rights noted:

> 79. … [T]he external, preferably judicial, a posteriori control of secret surveillance activities, both in individual cases and as general supervision, gains its true importance, by reinforcing citizens' trust that guarantees of the rule of law are at work even in this sensitive field and by providing redress for any abuse sustained. The significance of this control cannot be overestimated in view of the magnitude of the pool of information retrievable by the authorities applying highly efficient methods

[22] See, for instance, Hugo Rifkind, Banning encryption is foolish and illiberal (The Sunday Times, 8 May 2023), https://www.thetimes.co.uk/article/banning-encryption-is-foolish-and-illiberal-r2wcbl80d; Julian Hayes, End-to-end encryption proposals risk mistrust, injustice and dispute (The Sunday Times, 27 April 2023), https://www.thetimes.co.uk/article/online-safety-bill-end-to-end-encryption-mistrust-injustice-comment-nx2c3069s; Fiona Jackson, Could WhatsApp be BANNED in Britain? Boss of popular messaging app slams UK law that proposes to make end-to-end encryption ILLEGAL (The Daily Mail, 18 April 2023), https://www.dailymail.co.uk/sciencetech/article-11984303/Encrypted-messaging-services-sign-open-letter-against-Online-Safety-Bill.html; Alex Hern, WhatsApp and Signal unite against online safety bill amid privacy concerns (The Guardian, 18 April 2023), https://www.theguardian.com/technology/2023/apr/18/whatsapp-signal-unite-against-online-safety-bill-privacy-messaging-apps-safety-security-uk; Lindsay Clark, Wrong time to weaken encryption, UK IT chartered institute tells government (The Register, 18 April 2023), https://www.theregister.com/2023/04/18/wrong_time_to_weaken_encryption; Chris Vallance, Signal would 'walk' from UK if Online Safety Bill undermined encryption (BBC, 24 February 2023), https://www.bbc.co.uk/news/technology-64584001.

[23] PI, Defeating encryption: the battle of governments against their people (1 February 2017), https://privacyinternational.org/blog/674/defeating-encryption-battle-governments-against-their-people; PI, Ghosts in Your Machine: Spooks Want Secret Access to Encrypted Messages (29 May 2019), https://privacyinternational.org/news-analysis/3002/ghosts-your-machine-spooks-want-secret-access-encrypted-messages; PI, No, the UK Hasn't Just Signed a Treaty Meaning the End of End-to-End Encryption (1 October 2019), https://privacyinternational.org/news-analysis/3242/no-uk-hasnt-just-signed-treaty-meaning-end-end-end-encryption; Joe Mullin, The U.K. Paid $724,000 For A Creepy Campaign To Convince People That Encryption is Bad. It Won't Work. (EFF, 21 January 2022), https://www.eff.org/el/deeplinks/2022/01/uk-paid-724000-creepy-campaign-convince-people-encryption-bad-it-wont-work.

[24] Klaas and Others v Germany, App.No. 5029/71 (6 September 1978), para 56; Dragojević v Croatia, App.No. 68955/11 (15 January 2015), para 98; Roman Zakharov v Russia, App.No. 47143/06 (4 December 2015), para 249 ("The Court accepts that the requirement of prior judicial authorisation constitutes an important safeguard against arbitrariness"); Szabó and Vissy v Hungary, App.No. 37138/14 (12 January 2016), para 73; Big Brother Watch and Others v The United Kingdom, App.Nos 58170/13, 62322/14 and 24960/15 (25 May 2021) [GC], paras 350-354.

[25] Annual Report of the Inter-American Commission on Human Rights 2020, Volume II – Annual Report of the Office of the Special Rapporteur for Freedom of Expression, OEA/Ser.L/V/II Doc 28 (30 March 2021), para 58 ("[The lawful use of surveillance activities] should follow the requirements of prior judicial authorization and be strictly necessary and proportionate to the legitimate interests the State seeks to protect").

> and processing masses of data, potentially about each person, should he be, one way or another, connected to suspected subjects or objects of planned terrorist attacks…

More recently, in *Big Brother Watch and Others v. the United Kingdom*, the Grand Chamber of the European Court of Human Rights declared:

> [I]n order to minimise the risk of the bulk interception power being abused, the Court considers that the process must be subject to "end-to-end safeguards", meaning that, at the domestic level, an assessment should be made at each stage of the process of the necessity and proportionality of the measures being taken; that bulk interception should be subject to independent authorisation at the outset, when the object and scope of the operation are being defined; and that the operation should be subject to supervision and independent ex post facto review. In the Court's view, these are fundamental safeguards which will be the cornerstone of any Article 8 compliant bulk interception regime (see also the report of the Venice Commission, at paragraph 197 above, which similarly found that two of the most significant safeguards in a bulk interception regime were the authorisation and oversight of the process).[26]

Indeed, the double-lock mechanism was praised by the UK Government as one of the key human rights innovations of the IPA,[27] which for the first time sought to make clear the true powers claimed by intelligence and security services, under a democratic mandate.[28] Objective 1 suggests that the Government now seeks to walk back these much needed safeguards and return to a past surveillance regime that the former Independent Reviewer of Terrorism Legislation has described as "incomprehensible",[29] "undemocratic, unnecessary and – in the long run – intolerable".[30] In its Concluding Observations on the Seventh Periodic Report of the United Kingdom of Great Britain and Northern Ireland, the Human Rights Committee concluded that "*The State Party should: […] (c) Ensure that robust oversight systems over surveillance, interception and intelligence-sharing of personal communications activities are in place, including by providing for judicial involvement in the authorization of such measures in all cases*".[31]

Finally, we note that the removal of the safeguard of prior independent authorisation through Objective 1 will also have onerous consequences for the UK's ability to guarantee an effective protection of personal data for the purposes of an EU adequacy decision, as explained below.

Regarding the availability of redress mechanisms (i.e., the possibility to challenge any orders given by the Secretary of State to relevant operator(s) during the review process), the vague nature of the status quo requirement in Objective 1 makes the possibility for redress during the review process unclear. The European Court of Human Rights has found effective redress to be a crucial component of compliant surveillance regimes.[32] The importance of providing effective remedies, in the context of surveillance, was further underscored by the Court in *Big Brother Watch and Others v the United*

[26] Big Brother Watch and Others v The United Kingdom, App.Nos 58170/13, 62322/14 and 24960/15 (25 May 2021) [GC], para 350.
[27] UK Home Office, Investigatory Powers Act (1 March 2016), https://www.gov.uk/government/collections/investigatory-powers-bill - investigatory-powers-bill.
[28] T. Hickman, 'The Investigatory Powers Bill: What's Hot and What's Not?' U.K. Const. L. Blog (11th Dec 2015), https://ukconstitutionallaw.org/2015/12/11/tom-hickman-the-investigatory-powers-bill-whats-hot-and-whats-not.
[29] David Anderson, A Question of Trust: Report of the Investigatory Powers Review (June 2015), para 35, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/434399/IPR-Report-Web-Accessible1.pdf.
[30] Ibid.
[31] 17 August 2015, UN Doc CCPR/C/GBR/CO/7, para 24.
[32] See, for example, Kennedy v the United Kingdom, App.No. 26839/05 (18 May 2010), para 167.

Kingdom, where the Grand Chamber noted that "*an effective remedy should be available to anyone who suspects that his or her communications have been intercepted by the intelligence services, either to challenge the lawfulness of the suspected interception or the Convention compliance of the interception regime*".[33]

The lack of clear mechanism of redress would not only deprive individuals from finding out whether they have been affected by a formal notice under the IPA 2016 (as it might often be the case that there will never be a formal notice but only review processes), but it may also create difficulties for relevant operators to challenge any measures placed upon them by the Secretary of State during the so-called review process. The latter would contravene Article 13 of the Convention, which guarantees the availability at national level of a remedy to enforce the substance of the Convention rights and freedoms.[34]

OBJECTIVE 2

Objective 2 seeks to place an obligation on operators to cooperate during the consultation period preceding the serving of a formal notice, by sharing any technical or other information requested with the Home Office and/or the Judicial Commissioner. Combined with Objective 1 above, this change would mean that relevant operators would not only have to comply with the content of a future -but not guaranteed to ever materialise- notice, but they would also have to disclose -often sensitive- information about their systems or products.

Such disclosure obligations, in absence of a relevant warrant or prior independent authorisation, raise significant compatibility concerns with Article 10 of the Convention. This is because Objective 2 essentially seeks to limit the exercise of the discretion operators enjoy to accept or refuse to cooperate (and, accordingly, to provide or not provide any requested information) until a formal notice is served upon them. While the justification accompanying this government endeavour does not specify the types of information, we can safely assume that this will almost certainly also involve privileged technical information about the function of products and technologies deployed by operators, which would thus enjoy strong protections under business or trade secrets regulations.[35]

Recently, the UK Supreme Court recognised a doctrine of compelled speech.[36] The Court found that the compelled speech doctrine would not come into play only when a person is compelled to express religious or political views,[37] and even went further to suggest that the right against compelled speech is strongest "*when it would run counter to the underlying purpose or goals of the business or entity in question*".[38]

In the context of Article 10 claims, the European Court of Human Rights has repeatedly underlined that the "*necessity of any restriction on freedom of expression must be convincingly established*".[39] While national authorities do enjoy a certain margin of appreciation, this would be substantially limited in cases where the interests at stake are of utmost significance, such as the public and consumer interest of users. In *Sanoma Uitgevers B.V. v. the Netherlands*, the Grand Chamber underlined that "*orders to disclose sources potentially have a detrimental impact, not only on the*

[33] Big Brother Watch and Others v The United Kingdom, App.Nos 58170/13, 62322/14 and 24960/15 (25 May 2021) [GC], para 46.
[34] Rotaru v Romania, App.No. 28341/95 (4 May 2000), para 67.
[35] See, The Trade Secrets (Enforcement, etc.) Regulations 2018.
[36] Lee v Ashers Baking Company Ltd and others, [2018] UKSC 49.
[37] Ibid, para 55 per Lady Hale.
[38] J. Rowbottom, 'Cakes, Gay Marriage and the Right against Compelled Speech', U.K. Const. L. Blog (16th Oct. 2018) (available at https://ukconstitutionallaw.org/).
[39] Financial Times Ltd and Others v. the United Kingdom (2009), para 60.

source, whose identity may be revealed, but also on the newspaper or other publication against which the order is directed, whose reputation may be negatively affected in the eyes of future potential sources by the disclosure, and on members of the public, who have an interest in receiving information imparted through anonymous sources".[40] While that case dealt with compelled disclosure of journalistic sources, a similar analogy can be drawn in relation to telecommunications operators that deploy sophisticated technical processes to ensure the confidentiality and integrity of data, relying heavily on consumers' trust to do so.[41] In a recent online global consumer survey conducted by McKinsey, more than 50% of respondents said that they often or always make online purchases or use digital services from a company only after making sure that the company has a reputation for being trustworthy with its customers' data, while a substantial proportion of respondents indicated that they will take their business elsewhere if trust is violated.[42]

PI submits that the introduction of the disclosure obligations intended by Objective 2 would thus have a chilling effect on the rights of everyone using telecommunications services to express themselves online freely and securely.

OBJECTIVE 3

Objective 3 aims to strengthen any extraterritorial effects of the notice regime by making clear that the provisions of the IPA 2016 "*continue to apply to the operators to whom it was intended to apply, including those that have adopted more complex corporate structures*". In the context of the notice regime, this would mean that the obligations contained in a notice served by the Secretary of State upon the UK establishment of an operator would apply to the activities of that operator everywhere else (e.g., in the country of its main establishment or globally should the operator have a multinational presence).

While this is already the case with the existing provisions of the IPA 2016,[43] the text of the consultation mentions that "*the wider regulatory and commercial environment risks affecting the operational effectiveness of these notices given the current scope of the IPA*".[44] We note that some of the indirect implications that this Objective would have for both operators and users globally are being addressed in our comments on the other four Objectives. However, we would like to draw the attention of the UK Government to the following two considerations:

First, by their nature many telecommunications operators have an international presence. As such, they potentially can be subject to conflicting legal obligations imposed by multiple legal orders – from the US and the UK, to Russia and China and the European Union.[45] How those conflicts should be resolved remains the subject of significant ongoing discussion.[46] By expanding the extraterritorial effects of the notices regimes, the UK Government would be sending two problematic messages to

[40] Sanoma Uitgevers B.V. v. the Netherlands (2010), para 89.
[41] See, inter alia, Signal Support, 'Is it private? Can I trust it?', https://support.signal.org/hc/en-us/articles/360007320391-Is-it-private-Can-I-trust-it-; Robert E.G. Beens, The Role Of Digital Privacy In Brand Trust (Forbes, 8 January 2021), https://www.forbes.com/sites/forbestechcouncil/2021/01/08/the-role-of-digital-privacy-in-brand-trust.
[42] McKinsey, Why digital trust truly matters (12 September 2022), https://www.mckinsey.com/capabilities/quantumblack/our-insights/why-digital-trust-truly-matters.
[43] See, for example, Section 253(8) IPA 2016: "*A technical capability notice may be given to persons outside the United Kingdom (and may require things to be done, or not to be done, outside the United Kingdom)*".
[44] Home Office, Consultation on revised notices regimes in the Investigatory Powers Act 2016 (5 June 2023), https://www.gov.uk/government/consultations/revised-investigatory-powers-act-notices-regimes-consultation/consultation-on-revised-notices-regimes-in-the-investigatory-powers-act-2016-accessible-version.
[45] With regard to how the present proposal would impose conflicting obligations on operators, see also Comments on Objective 4 below.
[46] See, for example, IJPN, Internet & Jurisdiction Global Status Report 2019 (27 November 2019), https://www.internetjurisdiction.net/news/release-of-worlds-first-internet-jurisdiction-global-status-report.

the world: the first one is that any government is justified in reaching outside its borders to impose its will on services used by that government's citizens.[47] The second one is that the UK Government is somehow entitled to decide the fate of privacy and security for the data of every citizen in the world. For example, if the Government decides to undermine end-to-end encryption, by using the proposed changes to the notices regimes, then end-to-end encryption will also be weakened for citizens in states with authoritarian regimes and a weak rule of law.[48]

With communications channels that offer advanced security often being the sole means for lawyers, researchers, civil society, activists, human rights defenders, marginalised and vulnerable groups (including based on gender, religion, ethnicity, national origin or sexuality) and artists to avoid persecution, or even torture,[49] PI strongly urges the UK Government to restrain itself before setting a further troubling precedent that will likely also result in a violation of its obligations under international human rights law.[50] It should be recalled that, as the United Nations High Commissioner for Human Rights has underlined, "*where a State exercises regulatory jurisdiction over a third party that controls a person's information (for example, a cloud service provider), that State also has to extend human rights protections to those whose privacy would be affected by accessing or using that information*".[51] In particular, in relation to access to encrypted communications for journalists, human rights defenders and other categories at risk, the UN High Commissioner for Human Rights noted that "*encryption and anonymity tools are widely used around the world, including by human rights defenders, civil society, journalists, whistle-blowers and political dissidents facing persecution and harassment. Weakening them jeopardizes the privacy of all users and exposes them to unlawful interferences not only by States, but also by non-State actors, including criminal networks*".[52] In a similar vein, the UN General Assembly Resolution on the Safety of Journalists and the Issue of Impunity emphasized that "*encryption and anonymity tools have become vital for many journalists to freely exercise their work and their enjoyment of human rights, in particular their rights to freedom of expression and to privacy, including to secure their communications and to protect the confidentiality of their sources*".[53]

[47] PI, Submission to the Joint Committee on the Draft Investigatory Powers Bill (21 December 2015), https://privacyinternational.org/sites/default/files/2017-12/Submission_IPB_Joint_Committee.pdf, para 93.

[48] In July 2021, Forbidden Stories along with 17 media outlets around the world and the technical support of Amnesty International released a major investigation into the leak of 50,000 phone numbers of activists, lawyers, journalists and even world leaders, that had been selected as persons of interest by NSO client states, exposing possible targeting of NSO Group's Pegasus spyware in at least 11 countries: Azerbaijan, Bahrain, Hungary, India, Kazakhstan, Mexico, Morocco, Rwanda, Saudi Arabia, Togo, and the United Arab Emirates (UAE). Pegasus is a tool that relies on the exploitation of software vulnerabilities and has already been repeatedly exposed previously as having been used to unlawfully targeted human rights defenders, https://www.amnesty.org/en/petition/targeted-surveillance-human-rights-defenders. See also, Jamie Bartlett: Encryption is for everyone, not just extremists (Index on Censorship, 25 Aug 2017), https://www.indexoncensorship.org/2017/08/jamie-bartlett-encryption-extremists; Vernon Silver & Ben Elgin, Torture in Bahrain Becomes Routine With Help From Nokia Siemens (Bloomberg, 22 August 2011); BSR, Human Rights Impact Assessment: Meta's Expansion of End-to-End Encryption 64 (2022), https://www.bsr.org/reports/bsr-meta-human-rights-impact-assessment-e2ee-report.pdf.

[49] PI, Securing Privacy: Privacy International on End-to-End Encryption (September 2022), https://privacyinternational.org/sites/default/files/2022-09/SECURING PRIVACY - PI on End-to-End Encryption.pdf.

[50] See, UN General Assembly Resolution on the Safety of Journalists and the Issue of Impunity, UN Doc A/RES/74/157 (18 December 2019)("Emphasizes that, in the digital age, encryption and anonymity tools have become vital for many journalists to freely exercise their work and their enjoyment of human rights, in particular their rights to freedom of expression and to privacy, including to secure their communications and to protect the confidentiality of their sources, and calls upon States not to interfere with the use of such technologies and to ensure that any restrictions thereon comply with States' obligations under international human rights law."

[51] Report of the United Nations High Commissioner for Human Rights on the Right to Privacy in the Digital Age, UN Doc A/HRC/39/29 (3 August 2018), para 36.

[52] Ibid, para 20.

[53] UN Doc A/RES/74/157, 18 December 2019, para 15.

Second, in his 2015 report 'A Question of Trust', the then Independent Reviewer of Terrorism Legislation, David Anderson, noted that certain US service providers might be more likely to comply with requests from the UK if they were authorised by a judge.[54] He explained:

> 11.19. A number of major US companies, accustomed to the FISC procedure in the US, disliked the notion of authorisation by the Secretary of State and indicated to me that they would be more comfortable about complying with a warrant if it were judicially authorised, providing "another pair of eyes that is separate from the investigative apparatus" …
>
> 11.20. … Companies will reject requests which they feel are illegal in their host jurisdiction, or which they believe it would be unethical to meet, for example where the interests of a third country might be adversely impacted. I was shown evidence from a British agency that at one point in 2014 about 75% of the desired intelligence coverage for a particular operation could not be obtained from service providers.

Even if one assumes, for the sake of the argument, that US operators are satisfied with the current 'double-lock' mechanism and the prior authorisation by the Judicial Commissioners enshrined in IPA 2016, it is hard to see how the totally unchecked powers sought to be established by Objectives 1, 2 and 4, which are far from anything like a US judicial authorisation mechanism, could ever convince US operators to comply with the obligations imposed upon them.

OBJECTIVE 4

Objective 4 seeks, amongst others, to introduce a requirement for operators to give advance notice to the Secretary of State of relevant changes, including technical changes. While the proposal does not specify the sort of technical changes relevant operators would be expected to inform the Secretary of State about, these may include changes in the architecture of software, such as security updates, which are meant to fix vulnerabilities contained in software. Accordingly, the Secretary of State could then request operators to, for instance, abstain from patching security gaps with or without serving a formal notice, by virtue of the present Objectives.

We find Objective 4 extremely problematic. If adopted, it would undermine not only consumer trust but fundamentally threaten the integrity and security of data and digital infrastructure at a global level.

Software updates keep our devices secure, functional, compatible with the latest apps, and protected against known security vulnerabilities.[55] Out-of-date software on an otherwise functioning device can be a door to one's bank account or the intimacy of one's life, render a device unusable, or worst endanger safety and life, along with putting others at risk.[56] What past cyberattacks have underlined is that hoarding system vulnerabilities might have onerous consequences for citizens globally. For example, WannaCry was developed by hackers who effectively managed to exploit vulnerabilities

[54] David Anderson, A Question of Trust: Report of the Investigatory Powers Review (June 2015), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/434399/IPR-Report-Web-Accessible1.pdf.

[55] PI, An introduction to software updates (and why they matter) (29 October 2021), https://privacyinternational.org/explainer/4635/introduction-software-updates-and-why-they-matter.

[56] See, Saheli Datta Burton, Leonie Maria Tanczer, Srinidhi Vasudevan, Stephen Hailes and Madeline Carr, The UK Code of Practice for Consumer IoT Security: Where we are and what next (Department of Science, Technology, Engineering, and Public Policy, University College London, 2021), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/978692/The_UK_code_of_practice_for_consumer_IoT_security_-_PETRAS_UCL_research_report.pdf

stockpiled by the United States National Security Agency (NSA),[57] and seriously impacted European infrastructure operators in the sectors of health, energy, transport, finance and telecoms.[58] In the United Kingdom, which was among the first countries impacted by the cyber-attack, WannaCry had potentially serious implications for the National Health Service, leading to widespread disruption in at least 81 of 236 hospital trusts in England, with 19,000 medical appointments being cancelled, computers at 600 general practitioner surgeries being locked, and five hospitals having to divert ambulances elsewhere.[59] This potentially resulted in chaotic situations for patients, with sensitive personal data being encrypted or destroyed by the malware.[60]

Therefore, it is essential that device manufacturers, software vendors, and service providers -at a minimum- provide software security and key functionality updates for the expected lifespan of a product.[61] Unsurprisingly, consumers have widely recognised the importance of software security. A YouGov survey commissioned by PI in August 2022 shows that consumers expect their smartphones, computers, smart TVs and gaming consoles to receive security updates for a much longer period than what several manufacturers provide, leaving consumers with expensive tech that is vulnerable to cyberattacks.[62]

In light of the above considerations, two important legislative proposals are currently being discussed at EU level, one for a Directive on empowering consumers for the green transition,[63] and one for a European Cyber Resilience Act (CRA).[64] The former aims at enhancing consumer rights, particularly by ensuring that consumers obtain reliable and useful information on products, including on their lifespan. The latter has as one of its main objectives the creation of "*conditions for the development of secure products with digital elements by ensuring that hardware and software products are placed on the market with fewer vulnerabilities and ensure that manufacturers take security seriously throughout a product's life cycle*".[65]

Accordingly, Article 10(6) of the draft CRA, in its current form, states: *Manufacturers shall ensure that vulnerabilities of that product are handled effectively and in accordance with the essential requirements set out in Section 2 of Annex I during at least the expected product lifetime*.[66] Article

[57] Alex Hern, NHS could have avoided WannaCry hack with 'basic IT security', says report (The Guardian, 27 October 2017), https://www.theguardian.com/technology/2017/oct/27/nhs-could-have-avoided-wannacry-hack-basic-it-security-national-audit-office

[58] EU Agency for Fundamental Rights (FRA), Fundamental Rights Report 2018, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-surveillance-intelligence-services-vol-2_en.pdf.

[59] UK, National Audit Office, Department of Health, Investigation: WannaCry cyber-attack and the NHS (Report by the Comptroller and Auditor General, 27 October 2017) available at: https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf

[60] Patrick Sawer, Robert Mendick, Stephen Walter, Nicola Harley, NHS cyber chaos hits thousands of patients (The Telegraph, 13 May 2017), available at: https://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-chaos-hits-thousands-patients

[61] PI, BEST BEFORE DATE POLICY BRIEF: Device sustainability through long-term software support (September 2021), https://privacyinternational.org/sites/default/files/2021-10/Best Before Report Final_0.pdf.

[62] PI, Privacy International research shows that smart device security updates fail to meet consumers' expectations (20 October 2022), https://privacyinternational.org/press-release/4964/privacy-international-research-shows-smart-device-security-updates-fail-meet.

[63] European Parliament, Empowering consumers for the green transition (Legislative Observatory, 2022/0092 (COD)), https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2022/0092(COD)&l=en.

[64] European Parliament, Cyber Resilience Act (Legislative Observatory, 2022/0272(COD)), https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2022/0272(COD)&l=en.

[65] European Commission, Cyber Resilience Act (15 September 2022), https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act.

[66] European Parliament, DRAFT REPORT on the proposal for a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (Committee on Industry, Research and Energy, 2022/0272(COD)), https://www.europarl.europa.eu/doceo/document/ITRE-PR-745538_EN.pdf.

10(6) of the draft CRA, in its current form, goes on to require that manufacturers "*actively inform users when their product with digital elements has reached the end of its expected product lifetime and vulnerability handling requirements cease to apply*".[67] More importantly, Article 11 of the draft CRA, in its current form, imposes reporting obligations on operators to notify both any actively exploited vulnerabilities (Article 11(1)) as well as any significant incident having impact on the security of the product with digital elements (Article 11(2)) to the European Union Agency for Cybersecurity (ENISA).[68]

A requirement, such as the one sought by Objective 4, for operators to notify the Secretary of State in advance of any technical changes, including the patching of software vulnerabilities through the provision of security updates, would likely interfere with the contradicting obligations placed on operators by the aforementioned EU laws. As it would be either not technically feasible or reasonable cost-wise to jurisdictionally limit a UK Home Office request to not provide a security update to the UK only, operators will be faced with a dilemma to either choose to comply with either regime (likely the EU one as it wouldn't compromise their business model and at the same guarantee the security and trust of their users) or cease their operations in the UK, as some have already threatened to do should these proposals find legislative grounding.[69] Objective 4 would thus have detrimental consequences for both consumers and innovation in the UK.

In addition, PI wishes to draw the Government's attention to free and open-source software (FOSS). The latter includes major projects such as openSSL, which deploys a robust, commercial-grade, full-featured toolkit for general-purpose cryptography and secure communication,[70] and has been crucial for digital innovation not only because many critical elements of the Internet rely on it to operate, but also because it has enabled several communities and researchers.[71] Security is one of the key features that make FOSS indispensable, because its open nature allows for anyone to identify and correct errors or omissions that a software's original authors might have missed.[72] The maintenance of FOSS predominantly relies on its users and volunteers, who are responsible for undertaking any technical changes.[73] Unless the UK Government relies on the assumption that operators of FOSS will never be subject to a notice under the IPA 2016 or that the security of any FOSS has already been compromised (and thus there is no need to be made aware of any technical changes applied to it), it would be impossible to request FOSS operators to notify the Secretary of State in advance of any technical changes, particularly because the notification of such a change would be opaque to an individual developer.

OBJECTIVE 5

The aim of Objective 5 is to introduce a new statutory power for the Investigatory Powers Commissioner to renew notices that are already in place, once a 2-year period has elapsed. Neither the relevant IPA 2016 provisions nor the relevant Codes of Practice specify the duration of TCNs or NSNs. Section 256(2) of the IPA 2016 imposes an obligation on the Secretary of State to keep TCNs and NSNs under regular review, while paragraph 8.29. of the Equipment Interference Code of Practice states: *A review of a technical capability notice will take place at least once every two years once capabilities are in place*. However, the exact timing of the review is at the Secretary of State's

[67] Ibid.
[68] Ibid.
[69] Zoe Kleinmann, Apple slams UK surveillance-bill proposals (BBC, 20 July 2023), https://www.bbc.co.uk/news/technology-66256081.
[70] Amanda Brock, What is open source, and why does it matter today? (Open Access Government, 8 February 2022), https://www.openaccessgovernment.org/open-source-technology/129261.
[71] OpenSSL, https://www.openssl.org/.
[72] Opensource.com, What is open source?, https://opensource.com/resources/what-open-source.
[73] Synopsis, Open Source Software, https://www.synopsys.com/glossary/what-is-open-source-software.html.

discretion. Likewise, regarding NSNs, paragraph 3.23 of the National Security Notice Code of Practice states that a NSN "*remains in force until it is revoked by the Secretary of State*", while paragraph 3.25. states: *The exact timing of a review of a national security notice is at the Secretary of State's discretion. However, a review must take place at least once every two years*. PI is strongly concerned about the existing duration of TCNs and NSNs which appears to go far beyond 2 years while leaving a wide margin of discretion to the Secretary of State.

While the introduction of additional safeguards, such as the one intended by Objective 5, should be welcomed, it is vital that they are robust to prevent against abuse. To that end, PI would like to raise the following four points:

First, we believe that the 2-year period is too long to be regarded as the standard duration of a notice served under the IPA 2016. This is because, as the Equipment Interference Code of Practice also acknowledges, the "*communications market is constantly evolving*".[74] The review of a notice should therefore be at the latest within 6 months after the notice is formally served, considering that 6 months is also the default duration of many of the surveillance warrants under the IPA 2016.[75]

Second, the Government proposal does not indicate that terminating a notice would be one of the options available to the Judicial Commissioner. Objective 5 merely states: *The introduction of a statutory role for the Investigatory Powers Commissioner within a renewal process would help ensure the notices remain necessary and proportionate*.[76] While self-explanatory, it should be explicitly stipulated that the Judicial Commissioner must terminate a notice, if they consider that they no longer remain necessary and proportionate.

Third, it is not clear whether the Judicial Commissioner will be effectively reviewing whether the original reasons for serving the TCN or NSN still exist or whether they will be merely rubber-stamping the decision of the Secretary of State. The Government proposal appears to contrast the renewal process intended by Objective 5 against a 'pseudo-renewal' process which "*requires the full case for the notice overall to be put forward*".[77] It should be made clear that the Judicial Commissioner will be conducting a full review of the notice, including the reasons put forward by the Secretary of State to assess whether those still exist to justify a renewal of the notice. More importantly, it should be explicitly stated that, in their review of a notice, the Judicial Commissioner must apply the same approach taken by domestic courts in judicial review cases and not Wednesbury standards of review. This is the review threshold applied by Judicial Commissioner for the IPA related warrants and authorisations.[78] There exists no reason it should not be applied in the context of the notices regimes.

Fourth, for the reasons explained in our comments on the rest of the Objectives above, there is a significant risk that this safeguard will be rendered meaningless. If the serving of formal notices becomes obsolete due to the UK Government's unchecked reliance on endless review processes to impose the content of potential notices (without even obtaining a prior approval by the Judicial Commissioner), then the safeguard proposed under Objective would end up being applied in the case

[74] Equipment Interference Code of Practice (March 2018), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715479/Equipment_Interference_Code_of_Practice.pdf.
[75] See, Section 32(2)(b), Section 116(2)(b), Section 143(1), Section 162(1), Section 184(2)(b) and Section 213(2)(b) IPA 2016.
[76] UK Home Office, Consultation on revised notices regimes in the Investigatory Powers Act 2016 (5 June 2023), https://www.gov.uk/government/consultations/revised-investigatory-powers-act-notices-regimes-consultation/consultation-on-revised-notices-regimes-in-the-investigatory-powers-act-2016-accessible-version.
[77] Ibid.
[78] Advisory Notice 1/2018: Approval of Warrants, Authorisations and Notices by Judicial Commissioners (8 March 2018), paras 19-21, https://csrcl.huji.ac.il/sites/default/files/csrcl/files/20180308_ipco_advisory_notice_12018.pdf.

of notices that would obviously require a renewal (and perhaps are less controversial or human rights infringing).

IV. IMPACT OF THE PROPOSED OBJECTIVES ON EU ADEQUACY

An assessment of the compatibility of the proposed changes to the notices regime with the European Convention on Human Rights is not only vital for the purposes of ensuring the UK's compliance with its Convention obligations, but also relevant with regard to the current and any future EU adequacy decision governing the transfer of personal data between the UK and the EU. On 28 June 2021, the European Commission adopted two adequacy decisions for the United Kingdom under the General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LED).[79] The former is based on Article 45(1) GDPR which provides that transfers of personal data between the Union and a third country may take place where the Commission has decided that the third country "*ensures an adequate level of protection*".

As the Court of Justice of the EU (CJEU) has held, the level of protection required by Article 45 GDPR must be read in light of the provisions of the Charter of Fundamental Rights of the EU (CFREU).[80] Article 52(3) of the Charter stipulates that the rights guaranteed in the Charter correspond to the rights guaranteed by the European Convention on Human Rights and the CJEU has held that account must "*be taken of the corresponding rights of the ECHR for the purpose of interpreting the Charter, as the minimum threshold of protection*".[81]

In issuing the adequacy decisions of 28 June 2021, the European Commission relied heavily on the existence of safeguards under UK law. It underlined:

> In particular, the collection of data by intelligence authorities is, in principle, **subject to prior authorisation by an independent judicial body**. Any measure needs to be necessary and proportionate to what it intends to achieve. **Any person who believes they have been the subject of unlawful surveillance may bring an action before the Investigatory Powers Tribunal**. The UK is also subject to the jurisdiction of the European Court of Human Rights and **it must adhere to the European Convention of Human Rights as well as to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data**, which is the only binding international treaty in the area of data protection. These international commitments are an essential elements of the legal framework assessed in the two adequacy decisions.[82] (emphasis added)

Further, we note that in its 'Opinion 14/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the United Kingdom', the European Data Protection Board (EDPB) placed particular emphasis on the IPA 'double lock' mechanism and the existence of independent judicial oversight in the face of judicial commissioners, while it expressed concerns with regard to the existence of "*avenues for the exercise of rights for the data subjects concerned, and possible redress avenues offered to them in the context of equipment interference operations, especially when they take place in the context of urgency*

[79] European Commission, Data protection: Commission adopts adequacy decisions for the UK (Brussels, 28 June 2021), https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3183.
[80] See CJEU, C-311/18, Facebook Ireland and Schrems (16 July 2020), paras 99-101.
[81] CJEU, Joined Cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net and others (6 October 2020), para. 124.
[82] European Commission, Data protection: Commission adopts adequacy decisions for the UK (Brussels, 28 June 2021), https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3183.

leading to a derogation to the double-lock procedure".[83] Similar criticisms were also voiced by the European Parliament in its resolution of 21 May 2021.[84]

For the reasons explained in our comments on the Objectives above, PI submits that the proposed changes to the IPA notices regimes would very likely put both the current as well as any future EU adequacy decisions in jeopardy as the UK will not be able to guarantee an adequate level of protection for personal data, due to the lack or circumvention of fundamental rights safeguards intended by the proposed Objectives.

28 July 2023

Privacy International (PI)

[83] EDPB, Opinion 14/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the United Kingdom (13 April 2021), https://edpb.europa.eu/system/files/2021-04/edpb_opinion142021_ukadequacy_gdpr.pdf_en.pdf, para 166.
[84] European Parliament, Resolution of 21 May 2021 on the adequate protection of personal data by the United Kingdom (2021/2594(RSP)), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021IP0262.