Foreign Influence on Americans' Data Through the CLOUD Act

Before the Subcommittee on Crime and Federal Government Surveillance
of the Committee on the Judiciary

June 5, 2025

Testimony of
Caroline Wilson Palow, Legal Director and General Counsel,
Privacy International

On behalf of Privacy International (PI), thank you for the opportunity to testify about the impact of foreign surveillance powers, particularly those of the United Kingdom, on Americans' data and the CLOUD Act. Privacy International is a nonpartisan, U.K.-based charity that advocates globally against government and corporate abuses of data and technology. It exposes harm and abuses, mobilises allies, 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. PI has an office in London and is funded by foundation grants and individual donations.[1]

In this statement, I describe a troubling surveillance power that allows the U.K. Government to secretly order a U.S. company to undermine the security and privacy of its users worldwide. That power is enshrined in the U.K.'s Technical Capability Notice (TCN) regime, which I will detail here, along with how that regime purportedly has been applied to Apple, concerns about the wisdom and legality of the Apple TCN, and how the TCN regime and other countries' similar powers interact with the CLOUD Act. The current state of play threatens the privacy and security of Americans, and indeed people worldwide, by undermining the crucial protection of encryption.

[1] Details of PI's financials: https://privacyinternational.org/about/financials

The U.K.'s Technical Capability Notice Regime

The surveillance power at the core of today's discussion is the U.K.'s ability to serve a Technical Capability Notice (TCN) on a relevant operator, including companies providing telecommunications services, as enumerated in the U.K. Investigatory Powers Act 2016 (IPA). The following are the main components of the TCN regime:

What is a TCN? TCNs are orders, issued by the U.K. Government, which can be used to force operators to architect their systems to comply with other relevant surveillance authorizations under the IPA,[2] such as warrants authorizing interception[3] or hacking, authorizations for the collection of metadata, or bulk warrants that permit untargeted use of these powers. TCNs may require, *inter alia*, "the removal by a relevant operator of *electronic protection* applied by or on behalf of that operator to any communications or data" (emphasis added) or matters "relating to the security" of a system.[4]

Who can receive a TCN? A TCN can be given by a U.K. Secretary of State, often the Home Secretary, to a "relevant operator," which includes a postal or telecommunications operator. Most germane here, telecommunications operators are defined as those who offer, provide or control telecommunications services used by people in the U.K. Telecommunications services are broadly defined and can include phone and internet communications.[5]

What is the extraterritorial reach of a TCN? The definition of a relevant operator is broad enough to encompass service providers that are not based in the U.K., but merely offer services which are used in the U.K. This is made explicit in IPA section 253(8), which states a TCN "may be given to persons outside the United Kingdom (and may require things to be done, or not to be done, outside of the United Kingdom)." The U.K. thus claims the ability to serve TCNs on U.S.-based companies, among others. The U.K. Government recently doubled down on the extraterritorial application of TCNs by expanding the definition of the operators on which they could be served so as to "continue to apply to the operators to whom it was intended to apply, including those that have adopted more complex corporate structures."[6] This enhanced

---

[2] Investigatory Powers Act 2016 (hereinafter "IPA"), §253 (Eng.).

[3] Interception, as understood in the U.K., is broader than the American concept. U.K. interception warrants can authorize live wiretaps, such as permitted under the U.S. Wiretap Act, or access to stored communications, which would be authorized in the U.S. under the Stored Communications Act.

[4] IPA, §253(5).

[5] IPA, §261.

[6] *See* Investigatory Powers Act 2016 Consultation: Revised Notices Regime, June 2023, Objective 3, at 11:

definition became part of the Investigatory Powers (Amendment) Act 2024 (IPAA), which expands "telecommunications operators" to include those who control or provide a telecommunications system which is "used by another person to offer or provide telecommunications service to persons in the United Kingdom."[7]

What is the process for serving and challenging a TCN? The U.K.'s Secretary of State initiates the process of giving a TCN to an operator.[8] If the Secretary is considering serving a TCN, she must first consult with the operator who may be served and consider, among other things, the cost and feasibility of compliance.[9] Once the Secretary decides to serve the TCN, it must be approved by a Judicial Commissioner.[10] TCNs must be necessary and proportionate to their aim, as well as practicable to impose and comply with.[11] Once issued, the TCN is enforceable by injunction against operators inside and outside of the U.K.[12] Operators subject to a TCN may pursue an internal appeal, of sorts, by referring the TCN back to the Secretary for a second look, which includes consultation with a Technical Advisory Board, and approval by the head of the U.K. independent oversight body, the Investigatory Powers Commissioner.[13] In a change included in last year's IPAA, although not yet in effect, the operator must freeze any systems implicated by the TCN during this referral period, to avoid making "a change that, if implemented, would have a negative effect on the capability of the person to provide any assistance which the person may be required to provide in relation to any warrant, authorisation or notice issued or given under this Act."[14]

If a notice is upheld after referral, the process for challenging a TCN is less clear, although the Investigatory Powers Tribunal, a UK tribunal which hears challenges to the UK's investigatory powers and the actions of its intelligence agencies, has authority to provide redress to anyone who believes they have been the victim of unlawful action

---

https://assets.publishing.service.gov.uk/media/6475e2c0b32b9e000ca95e74/Revised_notices_regimes_consultation.pdf

[7] IPA, §261(10)(c).

[8] IPA, §253(1).

[9] IPA, §§255(2)-(4).

[10] IPA, §254. A Judicial Commissioner is a serving or retired senior judge who supports "the Investigatory Powers Commissioner in his oversight duties by providing independent authorisation of applications for the use of certain investigatory powers." Investigatory Powers Commissioner's Office, *Judicial Commissioners* (accessed June 2, 2025), at https://www.ipco.org.uk/who-we-are/judicial-commissioners/

[11] IPA, §253(1), (4).

[12] IPA, §255(10).

[13] IPA, §257.

[14] IPA §257(3B), once it comes into effect.

by a public authority using covert investigative techniques, including specifically TCNs.[15]

Are TCNs secret? An operator who receives a TCN "must not disclose the existence or contents of the notice to any other person without the permission of the Secretary of State."[16] Thus, an American company subject to a TCN cannot reveal even its existence to U.S. officials and oversight bodies, much less external security experts, non-profit organizations, or users who play crucial roles in vetting the legality and wisdom of such Notices, which can have profound effects on all of our security and privacy. The Secretary of State has the power to allow an operator to discuss a TCN or its provisions.[17]

Recent changes to the TCN regime. As noted throughout this section, in 2024 the U.K. amended the IPA to add certain provisions expanding the reach of TCNs. In addition to the changes already mentioned, the U.K. created a new form of notice called a "Notification Notice."[18] While the Notification Notice provisions have not yet come into effect, they will have serious consequences when they do. A Notification Notice, if served on an operator, would require that operator to notify the U.K. Home Secretary if it plans to make a "relevant change" to its systems. A relevant change is defined extremely broadly, with the clear intent of requiring subject companies to notify the Home Secretary if they plan to implement any privacy and security measures that could affect their ability to comply with any other surveillance requirements under the IPA.

The new power appears to be squarely aimed at innovations and updates to encryption technology as well as other security features.[19] In relation to the latter, during the legislative debates surrounding the Act, the U.K. Government denied that security patches could be subject to the notification requirement. It did not rule out that Notification Notices could be used to gather this information, however, stating instead that: "we cannot foresee a circumstance in which a security patch would have

[15] Regulation of Investigatory Powers Act 2000 (hereinafter "RIPA"), §65(5)(czi) (Eng.).
[16] IPA, §255(8).
[17] *Id.; see also* Interception of Communications Code of Practice, Dec. 2022, §§ 8.23-8.25 (Eng.), at https://assets.publishing.service.gov.uk/media/639879928fa8f5530be3004b/revised_Interception_of_Communications_Code_of_Practice_Dec_2022.pdf (detailing potential scenarios in which the Secretary of State may consider allowing the operator to discuss a TCN with external people or institutions).
[18] Investigatory Powers (Amendment) Act 2024 (hereinafter "IPAA"), §21 (Eng.), to become IPA, §258A.
[19] *See* Draft Statutory Instrument on The Investigatory Powers (Codes of Practice, Review of Notices and Technical Advisory Board) Regulations 2025, §3, available at https://www.legislation.gov.uk/ukdsi/2025/9780348270716/introduction (defining a "relevant change" for the purpose of notification as, *inter alia*, "a change in the relevant operators ability to lawfully provide the content of communications", but not including a change that "fixes a defect in installed software and leaves the intended functionality of the software unchanged").

such a sweeping effect on lawful access capabilities." Should such a circumstance come to pass, it is unclear whether the U.K. would exercise its unfettered power. Like TCNs, Notification Notices are served in secret with companies prevented from revealing their existence. They also lack the crucial safeguard of being approved by a Judicial Commissioner.

As the foregoing demonstrates, the TCN regime gives the U.K. Government the power to attempt to alter the systems of companies the world over, so long as they have even a tenuous connection to providing telecommunications services in the U.K. That power is effectively unlimited in its scope, potentially requiring the re-architecture of critical infrastructure that provides privacy and security for all of us.

The Apple TCN

On February 7, 2025, the Washington Post reported[20] that the U.K. Home Secretary had served Apple with a TCN. The TCN purportedly targets Apple's Advanced Data Protection (ADP) service, which is an optional security feature for Apple users providing end-to-end encrypted (E2EE) iCloud storage which only the Apple user, and not Apple itself, can unlock. More specifically, an Apple user who turns on ADP secures their iCloud data using keys controlled by the user, not Apple. The TCN reportedly has worldwide effect, requiring Apple to undermine the security of ADP for all its users, not just those in the U.K.

Apple has neither confirmed nor denied the existence of the TCN. On February 21, 2025, however, Apple announced that it would be withdrawing its ADP services for UK-based Apple users.[21] The service is no longer available to new users in the U.K. and existing users expect the ADP functionality to be withdrawn soon. It seems reasonable to deduce from this withdrawal that Apple has received a TCN targeting ADP.

Apple then reportedly initiated a challenge to the TCN before the IPT,[22] which as mentioned above, hears legal claims against certain UK surveillance powers including TCNs. But the shroud of secrecy continued, as Apple did not admit to its challenge, nor did the U.K. government. The IPT listed a closed hearing without identifying the

[20] Joseph Menn, *U.K. orders Apple to let it spy on users' encrypted accounts*, Wash. Post, Feb. 7, 2025, at: https://www.washingtonpost.com/technology/2025/02/07/apple-encryption-backdoor-uk/
[21] Zoe Kleinman, *Apple pulls data protection tool after UK government security row*, N.Y. Times, Feb. 21, 2025, at: https://www.bbc.co.uk/news/articles/cgj54eq4vejo
[22] Tim Bradshaw and Lucy Fisher, *Apple launches legal challenge to UK 'back door' order*, Fin. Times, Mar. 4, 2025, at: https://www.ft.com/content/3d8fe709-f17a-44a6-97ae-f1bbe6d0dccd

parties to the case.[23] This attracted much attention with multiple calls to open the hearing from media organizations, non-profit organisations, including PI, and a bipartisan group of members of Congress.[24]

Our collective suspicions were later confirmed when, on April 7, 2025, the IPT issued a judgment identifying Apple as the claimant that "filed a claim and a complaint in the Investigatory Powers Tribunal ("the Tribunal") raising issues as to the Secretary of State's powers to make Technical Capability Notices under the Investigatory Powers Act 2016."[25] The IPT's judgment is carefully worded in that it refers only to a generic challenge to "powers to make" TCNs and does not admit any further details about the purported TCN. It leaves open the possibility, however, that more details may be forthcoming as the challenge progresses.

The Washington Post's reporting, and the significant press follow-up, have provided us with the potentially unique opportunity to have a public debate about a specific application of a TCN because, as noted above, under the current state of the law, targets of TCNs themselves cannot reveal them.

Seizing that opportunity, the day before the IPT's closed hearing on Apple's challenge, PI and three co-claimants filed a public challenge to the TCN regime. PI's co-claimants are Liberty, another charity that defends fundamental human rights and freedoms in the U.K., and two individuals, PI Executive Director Gus Hosein and the director of the American Civil Liberties Union's Speech, Privacy, and Technology Project, Ben Wizner.

PI's complaint questions the legality of the TCN served on Apple as well as the TCN regime in general, alleging that the Apple TCN is ultra vires, disproportionate and lacks sufficient safeguards to be in accordance with the law. The IPT allows cases to proceed on hypothetical facts, which means neither Apple nor the U.K. Government need to admit the details of the TCN for PI's challenge to proceed. In its April 7th judgment, the IPT suggested PI's case may go forward in parallel with Apple's or proceed while Apple's is stayed.[26]

---

[23] Bill Goodwin, *Secret London tribunal to hear appeal in Apple vs government battle over encryption*, Computer Weekly, Mar. 11, 2025, at: https://www.computerweekly.com/news/366620363/Secret-London-tribunal-to-hear-appeal-in-Apple-vs-government-battle-over-encryption

[24] *See* Apple Inc v. Secretary of State for the Home Office (2025) UKIPTrib 1, available at: https://investigatorypowerstribunal.org.uk/judgement/apple-inc-v-secretary-of-state-for-the-home-department/

[25] *Id.*

[26] *Id.*

As of the date of this testimony, PI and its co-claimants have filed expert witness evidence with the IPT and are awaiting the U.K. Government's response to their complaint. The potential for further submissions in both PI's case and Apple's is still being considered by the IPT.

Security and Privacy Consequences of the Apple TCN

The Apple TCN exemplifies the potential for the TCN regime to have far reaching consequences that threaten our security and rights. It appears that Apple has been ordered to deliberately weaken ADP, which is an end-to-end encrypted (E2EE) service. E2EE is a fundamental security protection. It also plays an essential role in the protection of privacy, free expression, and freedom of association. Weakening E2EE can have a profound effect on our personal and professional lives.

Encryption plays a critical role in data privacy and security by safeguarding online communications and data, enabling free speech, and providing protection for financial and legal transactions, amongst other things. Indeed, encryption is often mandatory from a regulatory perspective for organisations in areas such as healthcare, education, finance and banking.

What distinguishes E2EE from other encryption methods is that the data is encrypted before it is transmitted from a user's device and decrypted only after reaching its intended destination. As the encryption and decryption of data sent and received occurs on users' devices, E2EE provides only the intended recipients – not even the communications service or data storage provider – with access to the content of the message. E2EE ensures that third parties, including the service providers themselves, cannot decrypt the data being transmitted or stored, as the decryption keys are not accessible to them. The provider of storage or communication services is not trusted with access to the data, not least because there is a risk of compromise, hacking or improper use by or through the provider's services.

Such issues are not hypothetical. By way of example, in August 2022, the New York Times reported that a Twitter employee was convicted of spying for Saudi Arabia.[27] The individual allegedly used his access at Twitter to gathered personal information of political dissidents to pass to Saudi Arabia for payment. Service providers may also be

[27] Kalley Huang and Kate Gonger, Former Twitter Employee Convicted of Charges Related to Spying for Saudis, N.Y. Times, Aug. 9, 2022, available at: https://www.nytimes.com/2022/08/09/technology/twitter-saudi-arabia-spying-ahmad-abouammo.html

the subject of hacking and data breaches, or legal proceedings initiated in states that do not respect fundamental rights.

My understanding is that ADP operates using E2EE. Under ADP, Apple does not have access to the keys needed to decrypt data covered by ADP (which is stored in encrypted form on its servers and while being transmitted over the internet). It is therefore impossible for Apple to access any such data. Once ADP is enabled, the user takes control of the key, providing end-to-end security for the data. Without ADP enabled, Apple retains the key used to encrypt the cloud storage. As Apple holds the key in this scenario, it can be compelled to disclose that key or the information protected by it, and that information is vulnerable to hacking of Apple's systems by bad actors.

As we do not know the details of the Apple TCN, we do not know if the U.K. Government is demanding Apple turn off ADP or asking for some form of "backdoor" allowing ADP to appear to remain available but with a way for the U.K. Government to gain access to the information it protects. Either way, using legal authority to undermine the security of E2EE has profound implications.

My understanding from technical experts, including one of my fellow panellists, is that it is technologically infeasible to have both effective E2EE and mechanisms for third-party access.[28] That is because the basis of E2EE's effectiveness is that only endpoint users can access the protected data. To enable anyone else's access creates an inherent vulnerability that can be exploited by bad actors, including both hostile states and non-state actors, such as criminal networks.

The U.K. Government has defended its TCN power by declaring that it would only facilitate the U.K.'s lawful access that is accompanied by robust, rights-protective safeguards. PI may disagree that the U.K.'s safeguards are as robust as claimed, but that is beside the point because our concern about TCNs is that once a backdoor is created, states with far less stellar records on human rights, such as Russia and China, could seek similar access through legal process. Or exploit the vulnerability created without following legal process. Either way, by demanding third-party access to data, files and other content protected by E2EE, governments interfere with strong encryption and necessarily make our increasingly digital societies less secure.

[28] *See, e.g.*, PI, *Securing Privacy: Privacy International on End-to-End Encryption*, at https://privacyinternational.org/report/4949/securing-privacy-end-end-encryption; Abelson H., et al., *Keys Under Doormats: Communications of the ACM* (2015).

This insecurity could affect the billions of people who daily use E2EE services. For example, WhatsApp, iMessage and Signal are popular E2EE messaging services. WhatsApp alone has three billion users.[29]

Governments also promote the use of end-to-end encryption. The Federal Cyber Defense Skilling Academy (CISA) provides public guidance that "highly targeted individuals", such as those in senior government or political positions, should "use only end-to-end encrypted communications."[30] Prior to the Apple TCN becoming public, the U.K. National Cyber Security Centre (NCSC) encouraged barristers and solicitors to use E2EE services, including ADP.[31] The European Data Protection Board (EDPB) and European Data Protection Supervisor (EDPS) agree, opining that "end-to-end encryption ('E2EE') is a crucial tool for ensuring the confidentiality of electronic communications, as it provides strong technical safeguards against access to the content of the communications by anyone other than the sender and the recipient(s), including by the provider."[32]

As Professor Ciaran Martin (formerly head of the U.K.'s NCSC which is part of the Government Communications Headquarters (GCHQ)[33]) has put it, the reality is that senior politicians and officials use, and need to use, ordinary and widely available E2EE products that are not subject to government-mandated backdoors: "these friends and colleagues are acting rationally, not hypocritically: their important work can, sometimes, be better protected in this way. That's why this revolution in digital security cannot, Canute-like, be wished away, any more than public key cryptography could be held back indefinitely… It is now a national and international imperative that our increasingly digital societies are increasingly digitally secure."[34]

---

[29] *See* Laura Ceci, *Number of monthly active WhatsApp users worldwide from April 2013 to March 2025*, Statista, May 5, 2025, at https://www.statista.com/statistics/260819/number-of-monthly-active-whatsapp-users/

[30] Cybersecurity and Infrastructure Security Agency (CISA), Mobile Communications Best Practice Guide, Dec. 18, 2024, at https://www.cisa.gov/sites/default/files/2024-12/guidance-mobile-communications-best-practices.pdf

[31] National Cyber Security Centre, *Cyber security tips for barristers, solicitors and legal professionals*, originally at https://www.ncsc.gov.uk/files/Cyber-security-tips-for-barristers.pdf , archived by the WayBackMachine, at https://web.archive.org/web/20241102140713/https://www.ncsc.gov.uk/files/Cyber-security-tips-for-barristers.pdf (accessed June 2, 2025).

[32] EDPB-EDPS, Joint Opinion 04/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, § 97 (adopted July 8, 2022), at https://edpb.europa.eu/system/files/202207/edpb_edps_jointopinion_202204_csam_en_0.pdf

[33] GCHQ is the U.K's intelligence, security and cyber agency, which is roughly equivalent to the U.S. National Security Agency (NSA).

[34] Ciaran Martin, *End-to-End Encryption: the (Fruitless?) Search for a Compromise*,

Everyone benefits from having a private sphere in which to communicate and develop our opinions and beliefs, as well as to enable economic activity.[35] Some people may have heightened duties of confidentiality or be at increased risk of unlawful surveillance, making the protections of E2EE essential. These people include law enforcement and government officials, journalists, researchers, lawyers, non-profits, activists, human rights defenders, marginalised and vulnerable groups.[36] The UN High Commissioner for Human Rights has highlighted the privacy risks posed by measures that undermine encryption and recommends 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."[37]

If the U.K. Government succeeds in maintaining this TCN against Apple, it is likely further TCNs targeting E2EE may follow. The U.K. Government has a long-held and recurring ambition to undermine E2EE.[38] For instance, such TCNs could be used to force Meta or Apple to remove or undermine the E2EE of WhatsApp and iMessage, respectively.[39]

E2EE is not the only security protection at risk, however. TCNs 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. The TCN power is ill-defined. The IPA includes a list of five potential obligations that may be specified in a TCN, including those relating to: (1) providing facilities or services, (2) an apparatus owned or operated by the target

---

Blavatnik School of Government, University of Oxford, Nov. 23, 2021, at 11, available at https://www.bsg.ox.ac.uk/research/publications/end-end-encryption-fruitless-search-compromise

[35] *See, e.g.*, Article 29 Data Protection Working Party, Statement of the WP29 on encryption and their impact on the protection of individuals with regard to the processing of their personal data in the EU (11 April 2018), https://ec.europa.eu/newsroom/article29/items/622229/en ; 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, § 21 (4 August 2022)

[36] PI, *Securing Privacy: Privacy International on End-to-End Encryption*, at https://privacyinternational.org/report/4949/securing-privacy-end-end-encryption

[37] *Report of the UN High Commissioner for Human Rights on the right to privacy in the digital age*, Aug. 4, 2022, UN Doc A/HRC/51/17, para 57(b).

[38] *See, e.g.*, PI, *Defeating encryption: the battle of governments against their people* , Feb. 1 2017, at https://privacyinternational.org/blog/674/defeating-encryption-battle-governments-against-their-people; PI, *Ghosts in Your Machine: Spooks Want Secret Access to Encrypted Messages*, May 29, 2019, at 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*, Oct. 1, 2019, at 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, Jan. 21, 2022, at https://www.eff.org/el/deeplinks/2022/01/uk-paid-724000-creepy-campaign-convince-people-encryption-bad-it-wont-work.

[39] *See* IPA, §253(5)(c) (explicitly permitting TCNs relating to the removal of "electronic protection").

operator, (3) the removal of "electronic protection applied by or on behalf of" the operator, (4) the security of a postal or telecommunication service, or (5) the handling or disclosure of any information.[40] But that list is non-exhaustive. In theory, the U.K. Government could issue a TCN for any action the Home Secretary considers "necessary for securing that the operator or another relevant operator has the capability to provide any assistance" in carrying out interception, hacking or acquisition of metadata as permitted under the IPA, so long as that requirement is "practicable" for the operator.[41]

The Apple TCN is thus not only a threat to the security of Apple's services, but to E2EE in general, and potentially, if the TCN regime continues to exist in its current form, to the security of telecommunications services worldwide.

Legality of TCNs

A TCN requiring the undermining of E2EE is not only bad policy, it also likely violates U.K. law. Indeed, the TCN regime is particularly problematic due to its lack of transparency, disproportionality, and extraterritorial reach.

Lack of Transparency. The Apple TCN remains officially secret because of the IPA's strict gagging provision, which states "[a] person to whom a relevant notice is given, or any person employed or engaged for the purposes of that person's business, must not disclose the existence or contents of the notice to any other person without the permission of the Secretary of State."[42]

The gagging provision is legally problematic when combined with the ill-defined nature of the TCN power, as discussed above. That broad power fails to provide the necessary accessibility and foreseeability required of surveillance powers by U.K. law.[43] It is hard to see how a TCN that is entirely secret, and based on an ill-defined power, could be considered reasonably accessible and foreseeable to those it most affects,

---

[40] IPA, §§253(5)(a)-(e); *see also* The Investigatory Powers (Technical Capability) Regulations 2018, 2018 No. 253, available at https://www.legislation.gov.uk/uksi/2018/353/made (describing, in more detail, obligations the Secretary of State has declared to be practicable to impose).

[41] IPA, §§253(1)(a), (4).

[42] IPA, §255(8).

[43] Under Article 8(2) of the European Convention on Human Rights (ECHR), which is incorporated into U.K law by the Human Rights Act 1998, an interference with Article 8 rights is permitted only if it is "*in accordance with the law*" and "*necessary in a democratic society*" to achieve one or more of the aims specified in Article 8(2). An interference is "*in accordance with the law*" if it is lawful under domestic law and "*compatible with the rule of law*", i.e. "*accessible to the person concerned and foreseeable as to its effects.*" *Podchasov v. Russia*, Application No. 33696/19 (European Court of Human Rights), Feb. 13, 2024, at 61.

which are the users of the service targeted. There is no way of knowing the nature of any TCN, when or in what circumstances it might be made, or how long it will be in force. This total secrecy also precludes other important safeguards that protect against arbitrary conduct, such as notification of those affected by the TCN after it is terminated.

The gag further frustrates a legitimate and robust policy debate about the use of this highly intrusive power – a debate we are only now able to have due to the luck of having an intrepid reporter at the Washington Post. It also means American companies like Apple are not able to reveal and discuss TCNs with Congress or other oversight bodies.

Disproportionality. In the U.K., a surveillance power is unlawful if it is disproportionate to its legitimate aim. That means, even if it is used to pursue a legitimate goal, such as targeted law enforcement investigations, it may still not be lawful if the harm it causes to security, privacy and other rights outweighs that benefit. Applying this to the context of E2EE, the European Court of Human Rights[44] has recognised that a statutory obligation to decrypt E2EE communications "risks amounting to a requirement that providers of such services weaken the encryption mechanism for all users" and thus is "not proportionate."[45] It went on to conclude that measures that "permit authorities to have access, on a generalised basis and without sufficient safeguards, to the content of electronic communications…" will necessarily impair "the very essence of the right to respect for private life."[46]

As an initial matter, because the Apple TCN has not been disclosed, we do not know if its purpose is legitimate. The U.K. Government is firmly maintaining its neither confirm nor deny position on the TCN, so has not revealed its whether it is to assist law enforcement or protect national security, much less a justification for why it should remain secret.

Even if the TCN has a legitimate aim, however, it is disproportionate. The reported TCN is blanket and indiscriminate in nature, affecting all of Apple's ADP functionality worldwide. There is no requirement that the relevant persons have been engaged in any wrongdoing or criminality: it is enough that they own an Apple device. This not only deeply impacts Apple users' privacy rights (as well as the rights of any other persons whose data is being stored by users on iCloud), but also their freedom of

[44] As a Council of Europe member-state, the U.K. abides by the European Convention on Human Rights, which is subject to the judicial supervision of the European Court of Human Rights. The Convention guarantees, among others, the right to privacy.
[45] *Podchasov*, Application No. 33696/19 at 79.
[46] *Id.* at 80.

expression. E2EE plays an essential role in enabling and facilitating free speech. It is invaluable to vulnerable groups, including minorities, journalists and political opponents (among others). And, as discussed in detail above, requiring a backdoor in ADP creates a vulnerability that puts the security of all users at risk from rogue nation states and criminals alike. Breaking E2EE in these circumstances is not justifiable.

Ultimately, the privacy and security implications of TCNs are profound because, as discussed above, a TCN can demand systemic change. That is, using a TCN, the U.K. Government can demand that operators alter their services in a way that may deeply affect all users. That cannot be proportionate.

Extraterritorial Reach. IPA section 253(8) states a TCN "may be given to persons outside the United Kingdom (and may require things to be done, or not to be done, outside of the United Kingdom)." This is bolstered by the definition of a relevant operator, which is broad enough to encompass service providers who are not based in the U.K., but merely offer services which are used in the U.K.

While the extraterritoriality of TCNs is not clearly a violation of U.K. law, it could result in targets of TCNs being faced with potential conflicts of laws. For instance, a European company may find itself struggling to comply with data protection obligations if a TCN requires it to undermine the security of its systems and not tell its users about that change. An American company might similarly be placed in the position of being forced to lie about the security of its products, a misrepresentation or omission which could be considered a deceptive trade practice. Undermining E2EE also squarely conflicts with American public policy such as the CISA's promotion of encryption as a strong security measure.[47]

TCNs and the CLOUD Act

Considering the TCN regime's significant impact on fundamental rights and American companies, several questions have been raised about the interaction of TCNs and the CLOUD Act. I address my understanding of that interaction in this section.

In some ways, the TCN regime and the CLOUD Act operate independently of each other.[48] As described above, the IPA includes exterritorial enforcement provisions that

[47] Cybersecurity and Infrastructure Security Agency (CISA), Mobile Communications Best Practice Guide, Dec. 18, 2024, at https://www.cisa.gov/sites/default/files/2024-12/guidance-mobile-communications-best-practices.pdf

[48] *See, e.g.*, PI, *No, the UK Hasn't Just Signed a Treaty Meaning the End of End-to-End Encryption*, Oct. 1, 2019, at https://privacyinternational.org/news-analysis/3242/no-uk-hasnt-just-signed-treaty-meaning-end-end-end-encryption

do not rely on the CLOUD Act. Thus, the U.K. claims the ability to serve a TCN directly on a U.S. company irrespective of the CLOUD Act.

The existence of the TCN regime and its potential impact on encryption, however, were raised by PI and others while the CLOUD Act was being drafted.[49] Despite these concerns, the CLOUD Act steers clear of encryption, touching on it only when requiring that Executive Agreements "not create any obligation that providers be capable of decrypting data or limitation that prevents providers from decrypting data."[50] At the time of the signing of the U.K Executive Agreement, the Department of Justice (DOJ) declared the CLOUD Act "encryption neutral". According to the DOJ, "[t]his neutrality allows for the encryption issue to be discussed separately among governments, companies, and other stakeholders."[51]

Yet TCNs may have significant effects on fundamental rights and American companies. We raised TCNs during the CLOUD Act negotiation because they are a core component of U.K. surveillance law. The goal of the CLOUD Act, as evidenced by its Congressional Findings, was to minimize conflicts of laws while preserving the "protection of privacy and civil liberties."[52] Allowing TCNs to be served on American companies creates a potential conflict of laws, as noted above, and severely infringes privacy and civil liberties.

Other provisions of the CLOUD Act are also implicated by the TCN regime. To enter into an Executive Agreement, a foreign government's domestic law must be assessed as to a number of factors.[53] Several of those factors require adherence to international human rights standards, including protection from arbitrary and unlawful interference with privacy and freedom of expression. Another factor demands the foreign government have "sufficient mechanisms to provide accountability and appropriate transparency regarding the collection and use of electronic data."[54] The TCN regime, especially as applied in the case of the Apple TCN, fails to satisfy any of these factors because, as alleged in our challenge and detailed above, (1) it is disproportionate and lacks the necessary qualities of accessibility and foreseeability, leading to an

[49] *See, e.g.*, Center for Democracy and Technology, *Cross-Border Law Enforcement Demands: Analysis of the US Department of Justice's Proposed Bill*, Aug. 17, 2016, at https://cdt.org/wp-content/uploads/2016/08/DOJ-Cross-Border-Bill-Insight-FINAL2.pdf
[50] Electronic Communications Privacy Act of 1986 (hereinafter "ECPA"), 18 U.S.C. §2523(b)(3).
[51] U.S. Dep't of Just., Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, April 2019, at 6, at https://www.justice.gov/archives/opa/press-release/file/1153446/dl?inline=
[52] CLOUD Act, Public L. No. 115-141, §102(6) (2018).
[53] ECPA, 18 U.S.C. §2523(b)(1)(B).
[54] *Id.* §2523(b)(1)(B)(v).

infringement of privacy and free expression, and (2) operates in complete secrecy, lacking all transparency.

Finally, once in place, the Apple TCN could open all iCloud data to U.K. Government access via the CLOUD Act. Once a backdoor is created in ADP, the U.K. could serve an overseas production order on Apple under the CLOUD Act seeking access to data protected by ADP. So long as the production order does not violate any of the CLOUD Act provisions, such as the prohibition on seeking data belonging to U.S. persons, then Apple would have few grounds on which to refuse to use the backdoor to access the requested data.

The only other country with an Executive Agreement, Australia, also has a Technical Capability Notice regime.[55] Australia's TCNs appear to be more narrowly defined than the U.K.'s in that the Australian Government asserts "nothing in this legislation can require industry to break encryption."[56] There is some debate, however, as to whether Australian TCNs may still raise security concerns or even permit access to E2EE data in a more targeted way.[57]

Furthermore, the European Union (EU) is negotiating an Executive Agreement.[58] While I am not aware of any EU country having a TCN-like regime, several countries and the EU itself have recently been considering measures that would undermine E2EE.[59]

---

[55] Austl. Gov't Dep't of Home Affairs, The Assistance and Access Act 2018, Jun. 5, 2023, at https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/data-encryption

[56] *Id.*

[57] *See, e.g.*, Peter Alexander Earls Davis, *Decrypting Australia's 'Anti-Encryption' legislation: The meaning and effect of the 'systemic weakness' limitation*, Computer Law & Security Review, Vol. 44 (April 2022), at https://www.sciencedirect.com/science/article/pii/S0267364922000073

[58] U.S. Dep't of Just., *Justice Department and European Commission Announces Resumption of U.S. and EU Negotiations on Electronic Evidence in Criminal Investigations*, Mar. 2, 2023, at https://www.justice.gov/archives/opa/pr/justice-department-and-european-commission-announces-resumption-us-and-eu-negotiations

[59] Sweden is currently considering legislation that could compromise encryption, *see* Global Encryption Coalition, Joint Letter on Swedish Data Storage and Access to Electronic Information Legislation, Apr. 8, 2025, at https://www.globalencryption.org/2025/04/joint-letter-on-swedish-data-storage-and-access-to-electronic-information-legislation/; France recently rejected a similar measure, *see* Electronic Frontier Foundation, A Win for Encryption: France Rejects Backdoor Mandate, Mar. 21, 2025, at https://www.eff.org/deeplinks/2025/03/win-encryption-france-rejects-backdoor-mandate; and the EU has been debating a regulation that would require scanning of E2EE communications, among other things, *see, e.g.*, Global Encryption Coalition, GEC Steering Committee Statement on 9 September Text of the European CSA Regulation, Sept. 16, 2024, at https://www.globalencryption.org/2024/09/gec-steering-committee-statement-on-9-september-text-of-the-european-csa-regulation/.

In light of the interactions between the TCN regime and the CLOUD Act, as well the existence of surveillance regimes in other countries currently in or negotiating Executive Agreements, effective protection of our security and rights may require consideration of whether the CLOUD Act's purported encryption neutrality is sustainable.