State Access to Encrypted Data in the UK: the 'Transparent' Approach

ABSTRACT

This article foregrounds four key powers through which the UK intelligence and police agencies (broadly referred to hereafter as 'law enforcement') may access encrypted communications and data. It is structured as follows. First, a brief overview of the ECtHR's jurisprudence on communications surveillance contextualises the overarching normative framework that must be translated into domestic law. The four powers are then discussed, both in legal and practical terms. The first two powers operate covertly, without the knowledge of the target. The latter two operate coercively, allowing police to demand individuals unlock encrypted data on penalty of prosecution. The article argues that the overall effect is to weaken encryption systems globally.

Introduction: a history of secrecy

According to a former Home Secretary, the UK boasts 'world-leading legislation that provides unprecedented transparency and substantial privacy protection' governing covert and coercive investigatory powers.[1] Whether or not one agrees, it is a reversal of the historical situation. For centuries the British government, under the symbolic authority of the Crown, acted as if it had unfettered power to intercept communications. No law was required; indeed legislation was regarded as a risky form of publicity. As the Home Secretary William Harcourt put it in 1882, 'the very essence of the power is that no account can be rendered. To render an account would be to defeat the very object for which the power was granted.'[2] The reasoning is simple: if they knew their private correspondence was under surveillance, targets would modify or stop their correspondence.

[1] Alan Travis, 'Snooper's charter' bill becomes law, extending UK state surveillance', *The Guardian* (London, 29 November 2016) <https://www.theguardian.com/world/2016/nov/29/snoopers-charter-bill-becomes-law-extending-uk-state-surveillance>, accessed 19 October 2019.
[2] UK National Archives, 'John Bull' Article on Working of Postal Warrants (HO 45/25960 1935).

This attitude was maintained until 1985. In 1979, police incompetence during a criminal trial led to the accidental disclosure of evidence derived from telephone tapping. In response, the defendant brought proceedings against the police.[3] The High Court rejected the claim, holding that the English common law recognised no general right to privacy; therefore no rights were violated by phone tapping. The claimant took his case to Strasbourg, where the European Court of Human Rights (ECtHR) found the UK in violation of the right to privacy under article 8 of the European Convention on Human Rights (ECHR). Having anticipated this outcome, the government introduced legislation in the form of the Interception of Communications Act 1985. It should be noted that the period in question saw the privatisation of the telecommunications branch of the General Post Office. Legislation governing law enforcement access to communication was not only born of concern for human rights, it served also to guarantee and legitimise state access to private communications previously under government control.[4]

The Interception of Communications Act 1985 was successfully challenged in the ECtHR following revelations about secret UK interception of bulk quantities of Irish telecommunications.[5] Long before the case was determined the law was drastically overhauled by the Regulation of Investigatory Powers Act 2000 (RIPA). While RIPA updated the law regarding covert surveillance powers based on intercepted communications, it also introduced powers for compelling the disclosure of passwords to unlock encrypted data. The same year, the Terrorism Act 2000 introduced permanent powers to detain and question travellers at UK ports, including search powers which extend to examining the content of encrypted devices.

In 2013, the Snowden disclosures revealed that government communications surveillance went beyond what was lawfully permitted under RIPA. On the basis of these revelations, a number of NGOs successfully sought declarations of incompatibility between domestic UK law and ECHR rights.[6] This prompted the government to avow previously undisclosed surveillance techniques and to introduce the mammoth Investigatory Powers Act 2016, called by its critics 'the snooper's

[3] *Malone v Metropolitan Police Commissioner* [1979] Ch 344.
[4] See also section 4 of the Official Secrets Act 1920; Bernard Keenan, *Interception: law, media, and techniques.* (LSE Theses Online, 2017), 216-217.
[5] *Liberty and Others v UK* App no. 58243/00 (ECHR, 1 October 2008)
[6] For key examples see *Liberty/Privacy International and Others v Secretary of State for Foreign and Commonwealth Affairs and Others* [2015] UKIPTrib 13_77-H_2; *Privacy International and Greennet and Others v The Secretary of State for Foreign and Commonwealth Affairs and GCHQ* [2016] UKIP Trib 14_85-CH.

charter'.[7] It is significant that all three landmark statutes concerning covert access to communications have followed unfavourable legal judgments against the UK. At the time of writing the legislation is under review in Strasbourg and it is possible that key sections will be found incompatible with the Convention.

The Convention

Under the ECHR, state parties to the Convention must make legislation giving meaningful effect to Convention rights. The ECtHR can, on application, review these rules and procedures and decide whether or not they are compliant. In 2018, the First Chamber of the Court conducted a comprehensive review of the requirements in respect of covert surveillance in *Big Brother Watch and Others v UK*.[8] The case primarily concerns the use of bulk data by law enforcement, but it contains the most recent restatement of the overarching principles that the Court has developed.

States may lawfully conduct surveillance activities that could interfere with the rights to privacy and freedom of expression,[9] provided they do so in accordance with a publicly accessible legal framework, which in itself is compatible with the rule of law. Under article 8(2), any action infringing upon privacy must be 'necessary in a democratic state', which has been developed by the ECtHR to mean that it must be proportionate to its ends and done in pursuit of a legitimate aim. The ECtHR has long recognised that surveillance does not only concern the right to privacy but also the right to freedom of expression, protected by article 10 of the Convention. However, privacy is generally taken as the referent when deciding cases as, in general, the same legal standards under article 8(2) apply to governing potential infringements upon freedom of expression under article 10(2). The protections seek to ensure that states can act, covertly if necessary, to defend against threats but cannot 'undermine or even destroy democracy under the cloak of defending it'.[10]

According to the court six requirements must be met for a state's legal framework to be compatible with the Convention. First, the legal framework must indicate the nature of powers that

[7] Liberty, 'The Snooper's Charter' <https://www.libertyhumanrights.org.uk/human-rights/privacy/snoopers-charter> accessed 1 June 2019.
[8] *Big Brother Watch and Others v UK* App nos. 58170/13, 62322/14 and 24960/15 (ECHR, 13 September 2018).
[9] Protected by Articles 8 and 10 ECHR.
[10] *Big Brother Watch* (n 8) [308].

may give rise to an infringement of rights; second, it must indicate categories of people liable to be affected by the powers; third, it must put time limits on the duration of operations; fourth, there must be procedures in place for selecting, examining, using and storing any information obtained as a result; fifth, there must be precautions for protecting that information when using it or when communicating it to other parties, including foreign government agencies; sixth, the law must state the circumstances under which stored information must be erased or destroyed.[11]

For the powers to be 'in accordance with the law', the legal framework must be clear enough for covert surveillance to be 'foreseeable'.[12] Foreseeability does not apply to the actual conduct of surveillance, as that would defeat the purpose. It means the law must be 'sufficiently clear [so as] to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures'.[13] Certainly, the rules and guidance cannot be withheld altogether (as they were in the past). The IPA and its attendant Codes of Practice explicate in much clearer terms than RIPA did the rules and provisions governing the surveillance powers of the police and intelligence services.

There must be a judicial body capable of investigating and ruling on violations of the law and providing an 'effective remedy' where violations occur. There must also be independent review and supervision. As affected individuals will not ordinarily know they are under surveillance, they cannot bring legal complaints on their own behalf; hence the oversight system must be independent, rigorous, and empowered to provide adequate and equivalent guarantees of compliance.[14] The UK currently aims to fulfil this requirement with oversight provided by the Investigatory Powers Commissioner's Office and a judicial body called the Investigatory Powers Tribunal.

The IPA, notably, does not prohibit any activities that were previously carried out by British police and intelligence services, whether lawfully or unlawfully. In fact, as we shall see, it expands certain powers with respect to communication providers while maintaining all existing capabilities. Its main achievement is to bring 'in from the cold' the functioning of activities that

[11] Ibid [307].
[12] Ibid [304]-[306].
[13] Ibid [306].
[14] Ibid [308]-[309].

were, prior to Snowden, top secret and officially disavowed, such as bulk data collection and analysis for intelligence purposes and computer hacking by GCHQ. In this respect it is primarily a work of clarification and de-obfuscation rather than of constraint and control, making these extensive powers 'in accordance with the law'. It is both a product and a target of ongoing human rights litigation, serving as an excellent case study for the proliferation of legal 'grey holes', areas of public law where exceptional powers become normalised.[15]

Oversight

The use of the powers contained in the Investigatory Powers Act and RIPA are subject to ongoing review by the Investigatory Powers Commissioner, who produces annual summary reports on how the powers and used and the number of instances recorded. Individuals can bring complaints to the Investigatory Powers Tribunal, which can assess individual cases as well as assess the general compatibility of UK legislation measured against ECtHR standards.[16] Powers granted under the Terrorism Act 2000 are reviewed by the Independent Reviewer of Terrorism Legislation, who also produces annual statistical reports. The specific role of these bodies in relation to each of the four encryption-related powers is discussed below.

It should be noted as a preliminary point that the appearance of independence of these bodies is necessarily compromised by their duty to uphold state secrecy in fulfilling their oversight roles. They are 'hybrid' organisations, not quite of the executive, staffed by members of the judiciary, yet not quite independent either.[17] For example, judicial commissioners conduct *ex ante* approval of ministerial decisions and conduct *post facto* reviews of the operations that follow – according to the previous body which was not engaged in approval but only review, this means 'marking their own homework'.[18] An intractable problem is that the substantive process of reviewing classified material cannot in itself be reviewed. Unlike normal judicial processes, the

[15] Cian C Murphy, 'Counter-Terrorism and the Culture of Legality: The Case of Special Advocates' (2013) 24 King's Law Journal 1 19–37; see also Eva Nanopoulos, 'European Human Rights Law and the Normalisation of the "Closed Material Procedure": Limit or Source?' (2015) 78 The Modern Law Review 6 913–44.
[16] Extensively discussed in *Big Brother Watch* (n 8).
[17] Paul F Scott, 'Hybrid institutions in the national security constitution: the case of the Commissioners' (2019) 39 Legal Studies 3.
[18] Joint Committee on the Draft Investigatory Powers Bill 'Written Evidence' 683 [16].

public cannot observe how assessments are made. The European Court of Human Rights has consistently found that the UK's oversight regime is Convention-compliant,[19] yet it is also the case that these same oversight bodies failed to detect several ways in which the activities carried out by GCHQ prior to the Snowden disclosures were incompatible with the Convention.

1. Interception of encrypted communications

The first method of accessing encrypted communications is covert interception. This section first sets out the general power of targeted interception, then turns to the power to order communication service providers to remove or to alter encryption protocols to enable effective interception.

Interception warrants

Under section 15 of the IPA, a targeted interception warrant authorises the person to whom it is addressed to secure the interception of any communication in transmission and to obtain any 'secondary data' pertaining to the targeted communications. Secondary data refers to systems data that is attached to or logically associated with the communication which, when separated from the content of the communication, reveals nothing of its meaning. The most obvious example is the metadata generated by and associated with the communication medium under consideration, although 'secondary data' is framed so as to encapsulate a broader range of potential data. The targeted communications and the method of interception must be described in the warrant. The warrant can also authorise or require disclosure of the 'product' obtained by interception to the addressee of the warrant.[20] It authorises 'anything which it is necessary to undertake in order to do what is expressly authorised or required by the warrant',[21] and any conduct carried in pursuance of the aims of the warrant.[22]

Applications for interception warrants may be made by, or on behalf of, the heads of nine different authorities including the intelligence services, major police forces, defence, and the

[19] (n 8).
[20] IPA s 15(2).
[21] IPA s 15(5)(a).
[22] IPA s 15(5)(b)-(c).

Revenue. Applications are considered by a Secretary of State who must make three assessments before issuing a warrant. First, they must be satisfied that the warrant is *necessary* on any of three grounds: the interests of national security, the purpose of preventing or detecting serious crime, or the interests of the economic well-being of the UK (so far as it is relevant to national security).[23] Second, the conduct must be *proportionate* to the aim. Third, there must be in place satisfactory arrangements for the safeguarding, disclosure, storage, and destruction of any information obtained by interception.[24]

The targets of an interception warrant may be a person, organisation, a single set of premises, or a group of persons who share a common person or carry on a particular activity. If the warrant is for a single operation or investigation it can cover a broader set of persons, organisations, or premises.[25] Warrants may also be issued for training and testing purposes.[26] Part 6 of the IPA contains provisions for bulk interception warrants, which target overseas-related communications by thematic description, but cannot take effect against platform-based encryption (as explained below).

If an application for an interception warrant is approved at the ministerial level it must be reviewed by a judicial commissioner before taking effect. The review considers the application's necessity and proportionality assessments, applying the principles used in judicial review. The standard of the review is a 'sufficient degree of care' to comply with section 2 IPA, which is the general duty to protect privacy against arbitrary interference.[27] If a judicial commissioner refuses to approve the decision to issue a warrant, they must supply written reasons to the decision-maker and, assuming the commissioner who conducted the review was not the Investigatory Powers Commissioner (the head of the Commissioner's body), the decision-making may send the application to the Commissioner.[28] The Commissioner can either confirm the original decision or make a fresh decision.

[23] IPA s 20(2)(a)-(c). In Scotland, a Scottish Minister may issue a warrant, but only where the grounds are limited to the prevention or detection of serious crime, see section 21.
[24] IPA s 19(1)(a)-(c), s 19(3)(a)-(c), see also s 53 and s 54 IPA.
[25] IPA s 17(1)-(2).
[26] IPA s 17(2)(c), (3).
[27] IPA s 23(1) and (2).
[28] IPA s 23(5).

Urgent interception warrants may be issued without judicial approval. A judicial commissioner must be informed, and must decide before the end of the third working day after the day of issue whether to approve the decision. A refusal will immediately cancel the warrant, with no possibility of renewal or review by the Commissioner, and the warrant's addressee must ensure that interception stops as soon as possible.[29]

If the target is an elected member of the Houses of Parliament, the Scottish Parliament, the Northern Irish or Welsh Assemblies, or a Member of the European Parliament elected in the UK, then the Prime Minister must be consulted.[30] Where the interception is concerned with material subject to legal professional privilege or where it concerns confidential journalistic material, extra scrutiny and attention is required.[31]

Mutual assistance warrants

International requests for communications intelligence from allied states are mediated via mutual assistance warrants.[32] For UK authorities, the warrants authorise or require the person to whom they are addressed to secure, by any conduct described in the warrant, assistance of a kind in the warrant in accordance with either an EU mutual assistance instrument or an international mutual assistance agreement.[33] In the other direction, they allow for the provision of assistance to the authorities of a country or territory outside the UK. The assistance may be of any kind described in the warrant in accordance with an instrument or agreement.[34] Anything obtained under the warrant by interception of communication may be disclosed to the addressee.[35] Although all necessary conduct required in securing these outcomes is authorised, including the collection of secondary data and communications not described in the warrant,[36] 'secondary data' may not be provided under a mutual assistance warrant. In October 2019, the Home Secretary Priti Patel

[29] IPA s 24(1)-(4), s25(2).
[30] IPA s 26(1)-(3).
[31] IPA s 27-28.
[32] IPA s 15(1)(c).
[33] IPA s 15(4)(a).
[34] IPA s 15(4)(b).
[35] IPA s 15(4)(c).
[36] IPA s 15(5).

signed a treaty with the United States to 'allowing UK law-enforcement agencies to demand data from US technology companies – with reciprocal access offered to US authorities'.[37]

In summary, interception warrants target specified communications.[38] All relevant telecommunications operators are compelled to facilitate access to the communications sought under a warrant. Encryption complicates the picture.

Intercepting encrypted communications

Following the Snowden revelations, strong end-to-end encryption became a marketing and reputational imperative for most internet-based communication service providers. On commercial mobile messaging platforms like Apple's iMessage, WhatsApp, Signal, and Telegram, variants of public key encryption are now automatically applied to protect messages and verify users' devices. The purpose of encryption is not to prevent the interception of communication but to render it pointless by encoding messages.

The rise of widespread encrypted communication was very much on the minds of British politicians during the passage of the IPA. In 2015, then-Prime Minister David Cameron said in the aftermath of a terrorist attack in Paris,

> 'We have always been able, on the authority of the home secretary, to sign a warrant and intercept a phone call, a mobile phone call or other media communications, but the question we must ask ourselves is whether, as technology develops, we are content to leave a safe space—a new means of communication—for terrorists to communicate with each other. My answer is no, we should not be, which means that we must look at all the new media being produced and ensure that, in every case, we are able, in extremis and on the signature of a warrant, to get to the bottom of what is going on.' [39]

[37] Sam Trendall, 'Home secretary signs agreement for access to US tech firms' data' *Public Technology* (London, 7 October 2019) <https://www.publictechnology.net/articles/news/home-secretary-signs-agreement-access-us-tech-firms%E2%80%99-data> accessed 30 October 2019.

[38] IPA Part 6 governs the interception of untargeted communications in bulk quantities, but as shall become clear, that power does not directly allow access to encrypted communications and is therefore outside the scope of this article.

[39] Adam Bienkov, 'David Cameron: Twitter and Facebook privacy is unsustainable' *Politics.co.uk*, (London, 30 June 2015), <https://www.politics.co.uk/news/2015/06/30/david-cameron-twitter-and-facebook-privacy-is-unsustainable> accessed 15 June 2019.

The implication was that the law should mandate the removal of encryption from communications, rendering these 'safe spaces' open to law enforcement.[40] That has come to pass via Technical Capability Notices (TCN). The broad function of a TCN is to ensure that when an interception warrant is issued, the technical infrastructure is in place necessary 'for securing that the operator has the capability to provide any assistance which the operator may be required to provide in relation to any relevant authorisation'.[41] Under RIPA, TCNs could be issued in order to facilitate interception, and could only be issued to public communication providers with over 10,000 'persons' using their services in the UK.[42] Documents published from the Snowden files include details of the 'Preston' system, used to implement interception warrants via hardware installed by the major communication providers of the UK.[43]

After the IPA the scope of potential subjects of a TCN is substantially broader. A TCN may now be issued to any communications operator, no matter how small, and can require them to facilitate not just interception but also the collection of communications data or the implementation of measures amounting to 'equipment interference', discussed below. Targeting encrypted communications is now a key function of TCNs. During the Committee stage of the passage of the IPA into law, amendments were proposed that would expressly prevent TCNs being used to undermine the use of encryption. Resisting the amendments for the government, Earl Howe said:

> 'law enforcement and the intelligence agencies must retain the ability to require telecommunications operators to remove encryption in limited circumstances—subject to strong controls and safeguards—to address the increasing technical sophistication of those who would seek to do us harm.'[44]

Under the IPA, a Secretary of State may issue a TCN where it is deemed necessary for technical reasons and where the conduct required is proportionate to the aims of the notice.[45] The

[40] Graham Smith, 'Back doors, black boxes and #IPAct technical capability regulations' (*Information Law and Policy Centre blog* , 10 May 2017) <https://infolawcentre.blogs.sas.ac.uk/2017/05/10/back-doors-black-boxes-and-ipact-technical-capability-regulations/> accessed 1 June 2019.
[41] IPA, s 253(1)(a).
[42] Regulation of Investigatory Powers Act 2000 (RIPA), s12.
[43] Ryan Gallagher, 'Facing Data Deluge, Secret U.K. Spying Report Warned of Intelligence Failure' *The Intercept* (New York, 7 June 2016) <https://theintercept.com/2016/06/07/mi5-gchq-digint-surveillance-data-deluge/> accessed 2 June 2019.
[44] Hansard HL Vol 774 Col 90 (13 July 2016).
[45] IPA s 253(1)(a),(b).

TCN may impose obligations or specify specific steps to be taken by the operator within a given period of time.[46] As with interception warrants, the necessity and proportionality assessments are subject to review and approval by a judicial commissioner.[47] While a TCN cannot require that encryption be removed from a specific communication, it can require communication operators to provide a facility that would allow access on request.

Technical practicalities must be considered alongside the normative concerns of necessity and proportionality. The formulation of this requirement in the legislation is convoluted: the Secretary of State must consider it reasonable to impose an obligation on an operator for the purpose of securing 'that it is (and remains) practicable to impose requirements… to provide assistance in relation to relevant authorisations', and 'that it is (and remains) practicable for those operators to comply with those requirements'.[48] The existence and contents of a TCN must be kept secret.[49] Overseas operators can be addressed with TCNs and can be required to take action outside the UK.[50] The Secretary of State must consult with an operator before making them subject to a TCN. They must consider the benefits of the notice, the likely number of users affected by it, the technical feasibility of compliance, the cost of compliance, and any other effect that it may have, particularly when considering the removal of 'electronic protection', i.e., encryption.[51] An operator may refer a TCN back to the Secretary of State for review.[52] On review, the Technical Advisory Board – a non-departmental government organisation made up of technical experts who advise the Home Secretary on whether or not specific obligations imposed on communication service providers are reasonable – must consider the technical requirements and costs, while a judicial commissioner must review the proportionality of the notice.[53] Both can hear representations from the Secretary of State and the service provider concerned before reporting their conclusions to the

[46] IPA s 253(2),(6),(7).
[47] IPA s 254.
[48] IPA s 253(4).
[49] IPA s 255(8).
[50] IPA s 253(8).
[51] IPA s 255(2),(3),(4).
[52] IPA s 257(1)
[53] IPA s 257(6)-(7). The Technical Advisory Board was established in May 2002 pursuant to section 13 of RIPA. The Board describes its work in annual reports, which are available via the government's website, see Technical Advisory Board, Latest Reports <https://www.gov.uk/government/latest?departments%5B%5D=technical-advisory-board> accessed 20 October 2019.

Secretary of State.[54] If the Secretary of State decides to confirm the notice rather than revoke or vary it, she must seek the approval of the Investigatory Powers Commissioner.[55] TCNs are enforceable by an application for a civil injunction (or specific performance under section 45 of the Court of Session Act in Scotland).[56]

More detail is found in the Regulations made pursuant to the IPA, which contains a list of obligations that a TCN may impose.[57] In relation to encryption, Schedule 8 of the Regulations allows the following obligations:

> *8. To provide and maintain the capability to—*
>
> *(a) disclose the content of communications or secondary data in an intelligible form where reasonably practicable;*
>
> *(b) remove electronic protection applied by or on behalf of the telecommunications operator to the communications or data where reasonably practicable, or*
>
> *(c) to permit the person to whom a warrant is addressed to remove such electronic protection.*

The differences allow for a range of approaches. One such approach does not target encryption *per se* but instead compels operators to facilitate the 'disclosure' of content by targeting authentication functions. This emerged as a preferred option for GCHQ in November 2018, when Ian Levy and Crispin Robinson, GCHQ officials, published an article on 'principles of access' to encrypted communications. They suggest that, rather than removing encryption, the software on a targeted device should be secretly modified so as to copy all targeted communications to GCHQ.

> 'It's relatively easy for a service provider to silently add a law enforcement participant to a group chat or call. The service provider usually controls the identity system and so really decides who's who and which devices are involved - they're usually involved in introducing the parties to a chat or call. You end up with everything still being end-to-end encrypted, but there's an extra 'end' on this particular communication. This sort of solution seems to be no more intrusive than the virtual crocodile clips that our democratically elected

[54] IPA s 257(8)(b).
[55] IPA s 257(1), s 258.
[56] IPA s 255(10)-(11).
[57] The Investigatory Powers (Technical Capability) Regulations 2018 SI 2018 No. 353.

representatives and judiciary authorise today in traditional voice intercept solutions and certainly doesn't give any government power they shouldn't have.'[58]

To understand this, a brief technical description of the principles of end-to-end encryption is necessary. Today, most encrypted digital communications use variants of a technique known as public key cryptography, or 'asymmetric' cryptography. An algorithm is applied to a large random number to derive from it a pair of large numbers that are mathematically related via a 'one way' function. One number is assigned as the 'public key' and the other as the 'private key'. Only the private key need be kept secret. The public key can be openly and safely disseminated. Anyone can encrypt a message using an intended recipient's public key. Once encrypted, only the private key can decrypt the message. User A writes to User B using B's public key; B responds using A's public key. Each can read the other's message but a hostile interceptor cannot. This means there is no need to exchange secret keys, unlike in 'symmetric' encryption systems where the same key is used to encrypt and decrypt messages.

The one-way principle also works in reverse: messages encrypted using a private key can only be decrypted using the paired public key. This allows senders to add 'digital signatures' to messages by combining the message with their private key. A receiver who knows the sender's public key can decrypt the signature with the public key to check that it was indeed made by the owner of the matched private key, and thus be assured that the content of the message has not been falsified or altered in transmission. Asymmetric encryption thus allows simultaneous security *and* verification, without the risk of interception that is always associated with transmitting a second key. Everyone in a communication system keeps their own private key safe and enjoys secure communication.

On smartphone messaging applications, this work takes place invisibly within the application. Each user's private key is generated and stored on the user's device. The corresponding public key is transmitted to the platform's user database. When one user contacts another, the platform delivers the receiver's public key, and *only that key*, to the sender's device for encryption,

[58] Ian Levy and Crispin Robinson, 'Principles for a More Informed Exceptional Access Debate', (*Lawfare*, 29 November 2018) <https://www.lawfareblog.com/principles-more-informed-exceptional-access-debate> accessed 3 June 2019.

which is carried out on the sender's device. Transmission is handled by the platform, but the platform itself has no way of decrypting the scrambled message. Only the private key stored on receiver's device can unlock it. All messages are encrypted during transmission, including in group chats with multiple members.[59] The key point is that while a platform like WhatsApp may receive an interception warrant requiring access to a user's messages, they have no access to the unencrypted text of the targeted messages.

GCHQ's proposal takes aim at the authentication function of public key cryptography. Taking Whatsapp as an example, the software uses the authentication capacity of public-key cryptography to allow users in all two-way conversations to verify that there is no unwanted third party, including WhatsApp itself, secretly included in the group. The application creates a 'security code', a long number generated by algorithmically combining the communicants' public keys, which is graphically represented by a computer-readable QR code and by a 60-digit string of numbers. One participant in a chat can physically scan the other's QR code using their devices, or one can read aloud the 60-digit string to the other over a telephone call. Provided the two security code matches, the conversation is secure.[60] Without this safety number system, users cannot guarantee that eavesdroppers are not present. GCHQ's plan modifies this security code protocol. The public keys of the users in a chat session targeted by an interception warrant would, as usual, still be delivered to each communicant's device so that all outgoing messages are fully encrypted. But another key would be secretly delivered. This secret key would be used by the users' devices to encrypt and transmit messages to law enforcement.[61]

In response to Levy and Robinson, an open letter from a coalition of privacy advocates and technology companies strongly condemned the 'ghost protocol' proposal.[62] The signatories, including Apple, Google, Microsoft, and WhatsApp, argue that while this may maintain encryption in transmission, by fatally undermining authentication it destroys overall systemic trust, regardless

[59] This is a schematic description. In practice, the protocols used are more complicated, see 'WhatsApp Encryption Overview: Technical White Paper' (*WhatsApp*, 19 December 2017), <https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf.> accessed 10 June 2019, 5.
[60] Ibid, 10.
[61] This is why a generally specified bulk interception warrant cannot be used to this end. The targets must be known in advance so that their chat sessions can be targeted for delivery of the secret government key.
[62] Sharon Bradford Franklin and Andi Wilson Thompson (and others), 'Open Letter to GCHQ on the Threats Posed by the Ghost Proposal' (*Lawfare*, 30 May 2019) <https://www.lawfareblog.com/open-letter-gchq-threats-posed-ghost-proposal> accessed 5 June 2019.

of the legal framework governing the use and oversight of the power. Once that trust is gone, it cannot be recovered, creating an immediate chilling effect for journalists, activists, lawyers, and others who depend on secure communications. Second, the technical steps are different for each platform, greatly increasing the complexity of implementation and multiplying the risk of creating unforeseen vulnerabilities which could be exploited by hostile actors. Third, research and investment into authentication services would be impacted. Fourth, creating backdoors for officials opens up the possibility of abuse, for example, allowing domestic abusers within law enforcement to stalk and manipulate victims. Fifth, platforms operate globally. If the UK government is allowed access to encrypted communications, there is little reason to refuse other governments. In short, encryption is either secured for everyone or it is secure for no one.

Nonetheless, the legal reality is that the legislation and regulations are in place, and GCHQ officials have publicly endorsed the 'ghost protocol' methodology. Clearly the government regards it as a proportionate and necessary step. We do not know if any TCNs to this effect have in fact been made, nor do we know whether or not the members of the Technical Advisory Board and the judicial commissioners would approve them. We do not know whether or not global communication platforms would comply with such notices. If they refused, we do not know whether or not the UK government would pursue enforcement action. But as a matter of law, platform-based encryption is not a barrier to the effective execution of an interception warrant. Thus the risks of being a target of interception while using encrypted platforms are formally the same as for unencrypted platforms.

2. User-applied encryption

Platform-based communications are vulnerable to TCNs because the company that provides the platform is ultimately responsible for the functioning of the encryption process. This is not the case with free-standing encryption software. To give three examples, open-source programmes like Pretty Good Privacy (OpenPGP) allows basic public key cryptography to be applied to text, internet traffic data can be encrypted using virtual private networks (VPNs), while software like The Amnesic Incognito Live System (Tails) combine different encryption and security

tools to maximise the security of online communication.[63] When dealing with strong encryption applied by users, interception is rendered ineffective. Law enforcement must instead seek to gain access to the user's devices that way seek to access targeted data in its decrypted form. To do this covertly entails hacking into devices and networks.

Equipment interference

The euphemism for computer hacking under the IPA is 'equipment interference'. Only in 2015 did the UK government 'avow' the practice of equipment interference, publishing a draft Code of Practice in response to the case of *Privacy International and Greennet and Others v The Secretary of State for Foreign and Commonwealth Affairs and GCHQ* before the Investigatory Powers Tribunal.[64] The applicants argued that using the broadly drafted sections 5 and 7 of the Intelligence Services Act 1994 to authorise intrusions into privacy via computer hacking was unlawful.[65] With no specific instances of hacking admitted by the government, the IPT hypothetically ruled that the practice would be lawful if done within the UK and following the publication of the draft Code of Practice. Any prior hacking would have been unlawful. The Tribunal refused to make any ruling on acts carried on outside the British Islands.[66]

Equipment interference (EI) is now governed by thirty-seven provisions in the IPA and a Code of Practice.[67] There are two kinds of EI that may be relevant to encryption: targeted and bulk EI warrants. A targeted EI warrant authorises or requires its addressee to obtain equipment data, communications, and any other information. 'Obtaining communications' is a broad and non-exhaustive activity that includes monitoring, observing, listening or recording a person's communications or other activities.[68] Equipment data is a broadly defined category of any data

[63] 'Presentation from the SIGDEV Conference 2012 explaining which encryption protocols and techniques can be attacked and which not' *Der Spiegel* (Hamburg, 28 December 2014) <https://www.spiegel.de/media/media-35535.pdf> accessed 10 June 2019.
[64] [2016] UKIP Trib 14_85-CH.
[65] Simon McKay, *Blackstone's Guide to the Investigatory Powers Act 2016* (OUP 2017) 113–115.
[66] This led to satellite litigation regarding the Tribunal's jurisdiction, see *R (on the application of Privacy International) v Investigatory Powers Tribunal and others* [2019] UKSC 22.
[67] Equipment Interference: Code of Practice 2018.
[68] IPA s 99(4).

associated with a communication that is not and does not reveal the semantic meaning of the content.[69] The Code of Practice holds:

> 3.2 Equipment interference describes a range of techniques used by the equipment interference authorities that may be used to obtain communications, equipment data or other information from equipment. Equipment interference can be carried out either remotely or by physically interacting with the equipment.
>
> 3.3 Equipment interference operations vary in complexity. At the lower end of the complexity scale, an equipment interference authority may covertly download data from a subject's mobile device when it is left unattended, or an equipment interference authority may use someone's login credentials to gain access to data held on a computer. More complex equipment interference operations may involve exploiting existing vulnerabilities in software in order to gain control of devices or networks to remotely extract material or monitor the user of the device.

The protocols for issuing a targeted equipment interference warrant are similar to those for issuing targeted interception warrants. Both authorise conduct carried out in accordance with a warrant. Only the intelligence services, Defence Intelligence, and law enforcement may apply for a targeted EI warrant. The intelligence services may apply on any of three grounds: national security, the economic well-being of the UK so far as relevant to national security, and the prevention and detection of serious crime. Defence Intelligence may only apply on the basis of national security and law enforcement only for the purpose of preventing or detecting serious crime, except in Northern Ireland where the PSNI may apply on the basis of national security.

To issue a warrant, the Secretary of State must consider that it is necessary for the statutory purpose and that it is proportionate to the aim,[70] and that satisfactory arrangements are in force to give effect to safeguards over the retention and disclosure of data.[71] An application will not be necessary or proportionate if what is sought could reasonably be achieved by other means.[72] As is the case for interception warrants, the warrant must be approved by a judicial commissioner. The

[69] IPA s 100(2)-(3).
[70] IPA s 102(1); s103(1); s104(1); s106(1).
[71] IPA s 102(1)(c), 103(1)(d), 104(1)(c), 106(1)(c).
[72] IPA s 102(7), 103(3), 104(2), 106(11).

procedure for refusal and review, and the process used in urgent cases, is identical to that described above in relation to interception warrants.[73] Again, there are special considerations for MPs, journalists, and material subject to legal professional privilege.

A targeted EI warrant may authorise the targeting of equipment defined by three broad categories: ownership, location, and use. Targeted equipment can be specified as belonging to, used by, or in the possession of a person, organisation, or group sharing a common purpose or carrying out a particular activity; or more than one person or organisation where the intended interference is for the purpose of a single investigation or operation. Similarly, if defined by location, the targeted equipment may be all equipment in a particular location, or more than one location where the interference is for the purpose of a single investigation or operation. If defined by use, it refers to equipment being used for either a particular activity or activities of a particular description. Warrants may also be issued for training and testing purposes.

In summary, the targeted EI warrant can be thought of as analogous to an interception warrant for cases where interception is unable to make available the material sought. This could be because law enforcement are seeking stored data rather than ongoing communications, but it could also be because the relevant communications have been strongly encrypted by the target by one or more of the above-discussed user encryption methods.

Bulk Equipment Interference

The intelligence services may apply for a bulk EI warrant to obtain overseas-related communications, information, or equipment data.[74] 'Overseas-related' means the information, equipment data, or communications pertain to individuals outside the UK, and includes obtaining equipment data that would or may assist in establishing the existence of such information or communication.[75] On issuing a bulk EI warrant the Secretary of State must be satisfied that the warrant is necessary for one of the three operational purposes of national security, the prevention or detection of serious crime, or the economic well-being of the UK so far as relevant to national security, and only if it for the purpose of obtaining information regarding the acts or intentions of

[73] IPA s 102(1)(d), 103(1)(e), 104(1)(d), 106(1)(d), 108(1)-(5).
[74] IPA s 178.
[75] IPA s 176(1)-(2).

persons outside the UK.[76] The conduct must be considered proportionate to the aim of the conduct.

The warrant must specifically refer to one or more of a list of 'operational purposes', and these must be purposes for which the examination of material obtained under the warrant is necessary, and the operational purposes must be necessary on any of the grounds that the Secretary of State considers the warrant to be necessary.[77] The list of operational purposes must be 'maintained by the heads of the intelligence services… as purposes which they consider are operational purposes for which material obtained under bulk equipment interference warrants may be selected for examination'.[78] A judicial commissioner must review the necessity and proportionality assessments and confirm that the operational purposes specified are purposes for which the examination of material gained via the warrant is necessary.[79] Protocols for issuing and reviewing urgent warrants are similar to those explained above in relation to urgent interception warrants.[80]

Bulk EI is an extremely broad power which may be utilised speculatively. A bulk EI warrant could target broad types of software and hardware, devices or networks, or anything else that interferes or alters with the operation of equipment. In a letter to the head of the Intelligence and Security Committee of Parliament, Dominic Grieve MP, the Minister for Security, acknowledged that although bulk EI was presented during the passage of the IPA as a power that would be used 'sparingly', in practice it will be deployed extensively in response to the proliferation of encryption tools. The letter admitted that the consequences of large-scale exploitation of security flaws in software and hardware cannot be foreseen.[81] As canvassed above, the systemic risks of this approach are profound.[82]

---

[76] IPA s 178(3).
[77] IPA s 178(1)-(3).
[78] IPA s 183(5).
[79] IPA s 179.
[80] IPA s 180-181.
[81] Jamie Doward, 'GCHQ boosts powers to launch mass data hacking' *The Guardian* (London, 8 December 2018) <https://www.theguardian.com/uk-news/2018/dec/08/gchq-bulk-hacking-hacking-human-rights-privacy-alarm> accessed 15 June 2019.
[82] Susan Landau, 'Highlights from Making Sense of Snowden, Part II: What's Significant in the NSA Revelations' (2014) 12 IEEE Security Privacy 1 63; Susan Landau, 'Making Sense from Snowden: What's Significant in the NSA Surveillance Revelations' (2013) 11 IEEE Security Privacy 4 54–63.

3. Compelled disclosure under RIPA

As well as covert methods, coercive powers can be used to force individuals to unlock encrypted communication devices or networks under threat of prosecution. Digital devices do not simply transmit and receive communications; they also, by default, store them. Where web-based communication services are used, devices generally store passwords and access keys in cookies, automatically logging in to accounts. Unlocking a smartphone or laptop computer can therefore provide law enforcement with access to a wide range of otherwise encrypted communications. Where law enforcement agencies come into possession of an encrypted device, it is expedient for them to be able to order someone to decrypt it. In the UK, such orders are made under section 49 RIPA. There are two potential targets: the user of the device or encryption key and the manufacturer of the device.

Section 49 notices

Although the word 'encryption' appears in the title to Part III of RIPA, the operative sections of the legislation refer to accessing 'protected information', defined in section 56(1) as 'electronic data which, without the key to the data (a) cannot, or cannot readily, be accessed, or (b) cannot, or cannot readily, be put into an intelligible form'. 'Protected information' is broader category than encrypted information. Encryption is a process by which the symbolic elements of a message are algorithmically transformed, but other modes of electronically protecting information exist, such as steganography, in which the protected message is disguised as other information (e.g. a digital image), or as non-information (e.g. as random noise).[83]

Where the police, the intelligence services, the National Crime Agency, or Her Majesty's Revenue and Customs take possession of any 'protected information', in any format, by any lawful means whatsoever then they may order anyone reasonably believed to have it to disclose the encryption key or decrypt the information by issuing a notice under section 49 RIPA. Potential modes of acquiring the information include: arresting a suspect, searching premises, interfering with

[83] David Kahn, *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*, (2nd edn, Scribner, 1996), chapter 4: 'On the Origin of a Species'; Friedrich L. Bauer, *Decrypted Secrets: Methods and Maxims of Cryptology*, (3rd edn, Springer, 2002), 8.

property including computer systems, intercepting communications in transmission, acquiring data from a service provider, being provided with the information by a source, or any lawful means.[84]

Before issuing a section 49 notice the investigating officer must gain 'appropriate permission' from a Circuit judge in England, a sheriff in Scotland, or a County Court judge in Northern Ireland.[85] Permission may be granted only where necessary in the interests of national security, for the purpose of preventing or detecting crime, or where it is in the interest of the economic well-being of the UK.[86] A section 49 notice authorises interference with both personal privacy and, potentially, the right against self-incrimination (discussed below). The judge must consider the proportionality of the notice, and be satisfied that there is no reasonably practicable alternative option to obtaining the information sought. Judicial authorisation is not required where a free-standing discretionary power to issue section 49 notices is specifically granted to investigators under a statutory search warrant, an interception warrant, or an authorisation for acquisition of communications data. The power may be added to such a warrant or authorisation after its initial grant. In doing so the authority issuing the warrant or authorisation must consider the necessity and proportionality of granting the power, place a time limit on the duration of the power, and give on-going consideration to its necessity and proportionality where it extends over a longer period.

A section 49 notice is issued either in writing or in a manner that produces a record of it having been given. The protected information sought must be described in the notice. The subject of the notice must be given a reasonable amount of time to comply. The notice must be limited in time.[87] Where the 'key holder' targeted by the notice is related to the 'protected information' as an employee or corporate official, the notice must be given to the most senior employee or official possible, unless doing so would risk compromising the purpose of making the notice by tipping off the target. Where the authorising decision-maker consents , and where it is practical to include it, a

[84] RIPA s 49(1)(a)-(e).
[85] RIPA Sch.2, (1).
[86] RIPA s 49(3); unlike the Investigatory Powers Act 2016, in RIPA the 'economic well-being' purpose limitation is not expressly connected to national security.
[87] RIPA s 49(4)(a)-(f).

'tipping off' provision may be added to a section 49 notice under section 54, making it an offence for any person subject to the notice to disclose that they have received a notice.[88]

A person complies with a section 49 notice either by turning protected data into an 'intelligible' form, or by disclosing the information sought in an intelligible form, or by disclosing the key to access the protected data in an intelligible form.[89] A senior officer can direct that the key itself must be if the purpose of the notice would otherwise be defeated.[90] Where a person no longer knows the key, they may satisfy the notice by providing any information that may assist the authorities to discover the key or otherwise make the information intelligible.[91] Knowing failure to comply with a section 49 notice is a criminal offence: in national security and child protection cases the maximum sentence on conviction is 5 years' imprisonment, it is 2 years for all other serious offences on indictment, and 6 months on summary judgment.[92]

Manufacturers

It is conceivable, if unlikely, that some manufacturers could be required by section 49 to include law enforcement access keys in their devices. On most communication devices, the user-entered passcode is not the encryption key used to encrypt data. A random key is used to encrypt stored data on the device, while the user key (sometimes called Key-encrypting Key, or KEK) is used to encrypt the random key. The KEK is the passcode entered to unlock the device. Recent smartphones generate KEKs based on users' fingerprints or facial dimensions. Because the device-encrypting key is different from the user's passcode key, a user can change their passcode multiple times without having to decrypt and re-encrypt the entire device each time. Changing the passcode simply re-encrypts the device-encrypting key to produce a new KEK. But this also means that it is possible to build in back-door access at the key-encrypting stage. The device-encrypting key could be encrypted twice: once with the user's passcode, and once with a factory-loaded law enforcement key.

[88] RIPA s 54; there are a number of defences included in section 54.
[89] RIPA s 50.
[90] RIPA s 51.
[91] RIPA s 50(9).
[92] RIPA s 53.

Mandating for 'back-door' access is not a new idea. The first 'Cryptowars' of the 1990s revolved in part around U.S. government plans to require computers to ship with 'Clipper Chips', based on a similar principle. But escrowing law enforcement keys in this manner would create a host of problems for globalised manufacturers; similar to those identified in respect of TCNs.[93] If it were to happen, section 49 notices would enable UK law enforcement to compel disclosure.

Self-incrimination

In practice, section 49 notices are often issued to suspects in criminal investigations where the police wish to investigate their communication history and the contents of their hard drives. This has led to high profile successful prosecutions. However, to force disclosure of information from a suspect risks infringing the privilege against self-incrimination. The issue was considered shortly after section 49 came into force in the case of *R v S and A*.[94] The appellants stood accused of conspiring with a suspected terrorist, H, to breach H's control order, a preventive security measure that severely restricts a subject's liberty and puts them under close surveillance. When the police raided A's house, they found an encrypted computer with the password half-entered by the defendant. S was arrested in possession of a computer containing encrypted material. Both were served with section 49 notices and both refused to comply. They sought to stay the prosecution on the basis of the right not to self-incriminate.

Rejecting the defendants' application on appeal, Lord Judge first drew a distinction between the materiality of the encryption key and the intentionality of the defendant.[95] He held that an encryption key is a material fact and, as such, 'exists separately from each appellant's 'will'.'[96] As the privilege against self-incrimination only concerns intentional statements, it cannot be engaged by section 49. Moreover, the court held that where the decrypted information does not reveal evidence of a crime then the privilege against self-incrimination cannot have been violated. Where the protected information is incriminating, the privilege against self-incrimination *may* be engaged

[93] Abelson, Anderson, Landau et al., 'Keys Under Doormats: Mandating Insecurity by Requiring Government Access to all Data and Communications' (*DSpace@MIT*, 7 July 2015) <https://dspace.mit.edu/handle/1721.1/97690> accessed 10 June 2016.
[94] *R v S and A* [2008] EWCA Crim 2177, [2009] 1 All ER 716.
[95] A distinction derived from the ECtHR in *Saunders v UK* [1996] 2 BHRC.
[96] *R v S and A* at paragraph 19.

by the fact that the defendant knew the key and was forced into revealing this knowledge. But it is only engaged if their knowledge is taken as evidence against the compelled person in legal proceedings in addition to the decrypted data.[97] If it is, the trial judge can consider whether or not to exclude the compelled evidence or the means of its discovery on the basis that the coerced evidence may be prejudicial to a fair trial.[98]

Sir Anthony May confirmed this approach in *Greater Manchester Police v Andrews*, noting '[p]rivilege against self-incrimination is not absolute and it is plain that [RIPA] does not intend that it should be. Section 49(2)(c) requires that the imposition of a disclosure requirement has to be proportionate to what is sought to be achieved.'[99] This means that any risk of infringing the privilege should be considered within the proportionality assessment carried out when the notice is initially granted or renewed. Given that the privilege concerns only the knowledge of the password and that its admissibility as evidence is a decision for a trial judge, this represents a low test in relation to making a section 49 notice.

As Simon McKay points out, this is markedly different from the position in the United States, where the forced disclosure of encryption codes is distinguished from a mere physical act and is regarded as compelled 'testimonial' evidence, violating the Fifth Amendment protection against self-incrimination.[100] U.S. case law draws a distinction between compelled disclosure of a physical key to a safe, which is legally permissible, and compelled disclosure of knowledge of a password, which is not. McKay considers it is likely that Strasbourg will align Convention law with US law on this question.[101]

However, even if the ECtHR were to treat passwords as testimonial knowledge rather than material facts, the Convention differs from the U.S. Constitution in that the former does not contain an express prohibition on self-incriminating evidence. Article 6, the right to a fair trial, is a qualified right. This means that determining a breach of article 6 in a particular case involving self-

[97] *R. v Hertfordshire CC Ex p. Green Environmental Industries Ltd* [2000] 2 A.C. 412 and *R. v Kearns (Nicholas Gary)* [2002] EWCA Crim 748; [2002] 1 W.L.R. 2815; recognised by the ECtHR in *Allen v United Kingdom* (18837/06) (2010) 51 E.H.R.R. 22.
[98] Under subsections 76(2), 78(1) or 82(3) of the Police and Criminal Evidence Act 1984.
[99] [2011] EWHC 1966, paragraph 27, see also *Brown v Stott* [2003] 1 A.C. 681; *Allen v United Kingdom*.
[100] *In re Grand Jury Subpoena to Sebastien Boucher*, No. 2:06-mj-91, 2009 WL 424718 (D. Vt. Feb 19, 2009), see also *United States v. Fricosu*, 841 F. Supp. 2d 1232 (D. Colo. 2012).
[101] Simon McKay, *Covert Policing: Law and Practice* (2nd edn, OUP 2015) 304 (8.87).

incriminating evidence involves a balancing approach. As the Court put it in the case of *O'Halloran v United Kingdom*, 'what constitutes a fair trial cannot be the subject of a single unvarying rule but must depend on the circumstances of the particular case'.[102] Article 6 rights are 'capable of being traded off against the public interest'.[103] Treating passwords as self-incriminating knowledge rather than as material facts alter the parameters of the balancing act in the accused's favour and may in some cases render the decrypted material inadmissible altogether. Yet this would remain a question to be decided in the trial context, weighed against the public interest in admitting the evidence.

4. Compelled disclosure under the Terrorism Act

So far, authorisation of the powers considered here included some form of necessity and proportionality assessment, thereby giving effect to the basic normative requirements of the ECHR. But now we turn to schedule 7 of the Terrorism Act. This controversial power, only applicable at ports, allows police to stop, question, search and seize property from anyone, without the need for reasonable suspicion and on penalty of prosecution. This includes the power to effectively compel disclosure of encryption keys in the course of questioning. As the Independent Reviewer of Terrorism Legislation Max Hill Q.C. notes, there are three common experiences amongst those who are subjected to this power: 'the obligation to answer questions; the taking of biometric data, and the temporary removal and downloading of the contents of digital devices, mostly mobile phones.'[104]

In 2013 David Miranda, the husband of the journalist Glenn Greenwald, was detained and questioned while transiting Heathrow Airport because his computer allegedly contained a copy of the cache of classified NSA documents provided to Greenwald by Edward Snowden. Mr Miranda was detained under schedule 7 of the Terrorism Act 2000, which provides at paragraph 2:

> 'an examining officer may question a person to whom this paragraph applies for the purpose of determining whether he appears to be a person who [is or has been concerned in the commission, preparation or instigation of acts of terrorism]'.

[102] *O'Halloran v United Kingdom* (2008) 46 EHRR 21.
[103] Andrew Ashworth, 'Commentary on *O'Halloran and Francis*' (2007) Criminal Law Review 900.
[104] Max Hill Q.C., *The Terrorism Acts in 2016: Report of the Independent Reviewer of Terrorism Legislation on the Operation of the Terrorism Acts 2000 And 2006*, (London 2018).

Officers at posts and borders may stop and make enquiries of any person entering or leaving the UK without any requirement that there is a reasonable suspicion for the stop. To give a sense of how broadly this applies, consider the Port Circulation Sheet that authorised his detention under schedule 7:

> 'We assess that MIRANDA is knowingly carrying material, the release of which would endanger people's lives. Additionally the disclosure, or threat of disclosure, is designed to influence a government, and is made for the purpose of promoting a political or ideological cause. This therefore falls within the definition of terrorism and as such we request that the subject is examined under Schedule 7.'[105]

All that is required is some connection to the broad concept of 'terrorism'. Paragraph 5 states:

> A person who is questioned under paragraph 2 or 3 must—
>
> (a)give the examining officer any information in his possession which the officer requests;
>
> (b)give the examining officer on request either a valid passport which includes a photograph or another document which establishes his identity;
>
> (c)declare whether he has with him documents of a kind specified by the examining officer;
>
> (d)give the examining officer on request any document which he has with him and which is of a kind specified by the officer.

This creates a broad power to demand the decryption of protected data. David Miranda told the BBC in an interview that he unlocked his electronic devices under threat of prosecution.[106] It is an offence under paragraph 18(1)(c) of schedule 7 to refuse to comply with requests made or duties imposed under it. On conviction a person can be fined or imprisoned.

The Court of Appeal subsequently found Miranda's treatment incompatible with article 10 ECHR, failing to adequately protect freedom of expression. The court recommended that if journalistic material is to be seized under schedule 7, then a mechanism for obtaining prior judicial

---

[105] *R (Miranda) v SSHD* [2016] EWCA Civ 6 [11].
[106] 'David Miranda: High Court Restricts Inspection of Data' (*BBC News,* 22 August 2013) <https://www.bbc.co.uk/news/uk-23790578>. accessed 28 June 2019,

authorisation should be introduced.[107] After the Miranda case the Code of Practice was updated to include safeguards where journalistic material is at stake. Paragraph 40 of the Code now states:

> 'examining officers should cease reviewing, and not copy, information which they have reasonable grounds for believing is subject to legal privilege, is excluded material or special procedure material, as defined in sections 10, 11 and 14 of the Police and Criminal Evidence Act 1984 (PACE)'.[108]

However, the fundamentally broad scope of the power remains intact.

Limits to Schedule 7

Miranda's case aside, the judiciary has been reluctant to constrain the use of Schedule 7. In *Rabbani v DPP*,[109] the claimant had been stopped several times and asked to unlock his phone and computer for inspection. Each time he refused. Eventually he was prosecuted for wilfully obstructing or seeking to frustrate a search or examination. He entered a guilty plea, but later appealed against his conviction, relying upon the updated Code of Practice. Mr Rabbani argued that the paragraph 40 protections should have applied to the confidential material he was carrying on behalf of the advocacy organisation Cage. This argument failed, suggesting that campaigners who challenge the UK government on matters deemed to be relevant to 'terrorism' may be freely intercepted under schedule 7.

Questions of privacy and of self-incrimination arising from schedule 7 were addressed in the case of *Beghal v DPP*.[110] Mrs Beghal was prosecuted for refusing to answer questions at a port during a period of detention lasting around half an hour. Like Mr Rabbani, she pleaded guilty but later sought to appeal her conviction on the grounds of an infringement of her right not to self-incrimination. She also raised article 8, arguing that in the absence of reasonable suspicion there were no objectively justifiable grounds for interfering with her privacy, therefore her detention failed the test of legality having no objective basis in law. She further invoked article 5 ECHR because her liberty was infringed with no lawful justification.

---

[107] R *(Miranda) v SSHD* [2016] EWCA Civ 6.
[108] Code of Practice for Examining and Review Officers under Schedule 7 to the Terrorism Act (2015) 19; section 11(1)(c) PACE defines journalistic material as 'excluded material'.
[109] R*abbani v DPP* [2018] EWHC 1156 (admin).
[110] *Beghal v DPP* [2015] UKSC 49; [2015] 3 W.L.R. 344.

The Supreme Court dismissed her appeal by a majority of 4:1. The Court, led by Lord Hughes (with Lord Wilson agreeing), noted that the power was originally created by the Prevention of Terrorism (Temporary Provisions) Act 1974, introduced in response to IRA bombing campaigns in England, and had consistently been deemed a useful power by the office of Independent Reviewer of Terrorism Legislation since its creation in 1984.[111] On the matter of self-incrimination, they held that schedule 7 abrogates the privilege. Although it is a right 'firmly established' in law, schedule 7 would be 'nugatory' if it did not implicitly nullify its operation.[112] On article 8, the issue was divided into the question of legality – measured by the inclusion of adequate safeguards to prevent abuse – and the question of proportionality. On legality, Lord Hughes listed ten factors by which the power is constrained in its application, including the fact that it occurs only at ports, the need to keep records, and that the powers are subjected to *post facto* independent review. While officers do not require objective grounds for suspicion when making stops, this does not mean there are inadequate safeguards or that the power is not in accordance with the law.[113] Thus the majority thus took a systemic approach, finding that proportionality,

> '…depends in the end on the balance between the level of intrusion for the individual and the value of the power in community purpose served. It is common ground that the State is entitled to a generous margin of judgment in striking this balance. The importance for the public of the prevention and detection of acts of terrorism can scarcely be overstated and the level of risk of such acts is at least as high now as it has been at any time in the 40 years since these powers were introduced, though of course the sources of the threats have changed from time to time.'[114]

To require the authorities to show reasonable suspicion would restrict the utility of the power. The 'comparatively slight' intrusion into her privacy was thus held proportionate to the ends sought.[115] In relation to the interference with liberty under article 5 ECHR, the majority held that it

[111] Ibid [14]-[16].
[112] Ibid [64].
[113] Ibid [43]-[44].
[114] Ibid [48].
[115] Ibid [50]-[51].

was only 'barely' engaged because of the short period of time of her detention,[116] but held it would be lawful to detain a person for however long is required to complete lawful processes under schedule 7; and that sometimes this would be longer than strictly necessary.[117] Thus, her detention was held not disproportionate when weighed against the objective needs of security.

Only Lord Kerr dissented. First, on the matter of legality, he held that the broad scope of the power means its use cannot be in accordance with the law, because the 'opportunity to exercise a coercive power in an arbitrary or discriminatory fashion is antithetical to its legality.'[118] Without the need for reasonable suspicion, 'there is simply no material on which a judgment as to whether they are being used proportionately can be made'.[119] Lord Kerr was particularly critical of what he took to be the majority's implied position that counter-terrorism measures are automatically justified by their utility and efficacy in stopping terrorism even if no reasons are required to justify their use against particular individuals.[120] By this logic, he noted, any infringement of rights in the name of counter-terrorism would *always* be proportionate. But the 'proportionality of a measure is not to be determined by its efficacy in fulfilling its objective'.[121] Finally, he said that the mere absence of a prosecutorial investigation at the moment of interrogation is insufficient to protect against infringement of the right not to self-incriminate. Only where there is a binding guarantee that any information divulged will not be subsequently used in a prosecution should the application of article 6 ECHR be excluded.[122] Lord Kerr's reasoning gives slim hope that some meaningful limitation may be placed on schedule 7 powers in future. For now, UK ports are a zone of exception in which normal limits on state power are suspended and individuals can be compelled to reveal encrypted information.

---

[116] Ibid [53].
[117] Ibid [55].
[118] Ibid [93].
[119] Ibid [106].
[120] Lord Neuberger and Dyson respond to Kerr noting that the unpredictability of the use of sch. 7 stops is part of their strategic value, [77].
[121] Ibid [111].
[122] Ibid [118].

Conclusion

The web of powers canvassed here are all based on legislation. They have been greatly elaborated and elucidated since the Snowden revelations. Generally, these powers are limited by necessity and proportionality, which have been broadly interpreted by the courts. Exceptionally broad powers apply at ports, where any connection to 'terrorism', even the indirect possibility that journalistic material may somehow end up aiding terrorism, is enough to mandate the forced decryption of any devices in the subject's possession. All of these powers are subject to quasi-secret oversight processes.

Overall, it is hard to resist the conclusion that the primary function of the law and the oversight system is to publicise these powers and thereby ensure they are formally 'in accordance with the law'. Assessments of necessity and proportionality are taken secretly by ministerial and official actors. The legal framework ultimately guarantees that the state is empowered to gain access to information that it suspects is necessary for security purposes. The inevitable impact is to weaken encryption standards and systemic trust for everyone.