The evolution of elucidation: the Snowden cases before the IPT

abstract

In 2018 the European Court of Human Rights found that the UK's Investigatory Powers Tribunal is an 'effective remedy' when it comes to reviewing the compatibility of the UK's domestic legal framework governing the interception of communication and other communications surveillance powers with the requirements of the European Convention on Human Rights. In particular, the Court praised the Tribunal's 'elucidatory function', which it performed during a series of cases that arose in the aftermath of Edward Snowden's disclosures in 2013. This article analyses and historicizes the elucidatory function by comparing it with previous cases where the High Court and the IPT resolved questions of law arising from similar problems. Using insights derived from systems theory, the article argues that the elucidatory function evolved as a containment measure in response to unexpected crises of control over classified information. The procedure resolves conflicts between secrecy, security, and the publicity required by the law itself.

Keywords *Big Brother Watch and Others v. the United Kingdom* [2018] ECHR 722; *Big Brother Watch and Others v United Kingdom* [2021] ECHR 439; *Liberty v GGHQ* [2015] 3 All E.R. 212, [2015] 2 WLUK 215; *Belhadj v Security Service,* [2015] 4 WLUK 62; surveillance; Article 8 ECHR; Secrecy; Investigatory Powers Tribunal; Elucidation.

Author Dr Bernard Keenan, Lecturer in the School of Law, Birkbeck College

Acknowledgments This article began during my doctoral studies as a set of observations of open hearings before the Investigatory Powers Tribunal. I wish to thank Jude Bunting, Eric Kind, and Ben Jaffey QC for their insights into the Tribunal's processes, and my supervisors, Conor Gearty and Alain Pottage, for encouraging me to pursue the issue further. Thanks also to Daniella Lock,

Ewan Smith, Bo Bottomley, and Peter Goodrich for their valuable comments on earlier drafts, to Tom Poole and the editors at the MLR, and to the anonymous reviewers for their excellent feedback and suggestions.

*

In *Big Brother Watch v UK*, the First Chamber of the European Court of Human Rights (ECtHR) gave judgment on a joined application challenging the compatibility of the UK's domestic legal framework with the requirements of the European Convention on Human Rights (ECHR). The applications stemmed from the 2013 revelations by American whistle-blower Edward Snowden of surveillance powers operated by the UK's signals intelligence agency, Government Communications Headquarters (GCHQ).[1] Relying on Article 8 (the right to respect for family and private life), the applicants challenged the adequacy of the UK's legal regime concerning those powers, specifically in respect of bulk interception of communications, intelligence sharing with foreign powers, and the acquisition of metadata from communications service providers. Two of the three applicants complained about the lack of specific protection for journalists and NGOs under Article 10 (freedom of expression). The domestic regime for challenging such measures before the specialised Investigatory Powers Tribunal (IPT) was challenged under Article 6 (the right to a fair trial), while Article 14 (prohibition of discrimination) was invoked in combination with Articles 8 and 10 because the bulk interception regime is more likely to intercept and examine the communications of people located outside the British Islands than of those within.

---

* Unless otherwise stated, all URLs were last accessed 9 November 2021.

1 *Big Brother Watch and Others v. the United Kingdom* [2018] ECHR 722; the joined cases were *Bureau of Investigative Journalism and Alice Ross v. the United Kingdom* (no. 62322/14) and *10 Human Rights Organisations and Others v. the United Kingdom* (no. 24960/15). For a full analysis, K Hughes, 'Mass Surveillance and the European Court of Human Rights' (2018) 6 European Human Rights Law Review 589.

In its Chamber judgment of 13th September 2018, the Court found by a majority that bulk interception powers are in principle compatible with the Convention, but that the UK's regime in force at the time of the applications fell short of the requirements of Article 8. The law had provided insufficient oversight of the process for selecting bearers for interception and selecting intercepted communications and metadata for examination. Similarly, the regime for obtaining metadata from communication service providers contained inadequate safeguards. Article 10 was violated as there were insufficient safeguards for the protection of confidential journalistic material. The intelligence sharing regime was held to comply with the Convention, and the complaints under Articles 6 and 14 were unanimously held to be ill-founded. The Grand Chamber's judgment of May 2021 largely mirrored the First Chamber's findings, holding that the bulk interception regime was deficient, but intelligence sharing had sufficient safeguards in place to protect against abuse. Because the Article 6 complaint was resolved unanimously by the First Chamber, the Grand Chamber did not consider the IPT.[2]

This article departs from the First Chamber's unanimous findings regarding the IPT. The Tribunal was found to constitute an effective remedy under Article 13 for the purpose of assessing the compatibility of domestic law with the requirements of the Convention, and its procedures for

---

[2] *Big Brother Watch and Others v United Kingdom* [2021] ECHR 439. For detailed commentaries on the Grand Chamber judgment, E Watt, 'Much Ado About Mass Surveillance – the ECTHR Grand Chamber 'Opens the Gates of an Electronic "Big Brother" in Europe' in Big Brother Watch v UK' (28 June 2021) Strasbourg Observers at https://strasbourgobservers.com/2021/06/28/much-ado-about-mass-surveillance-the-ecthr-grand-chamber-opens-the-gates-of-an-electronic-big-brother-in-europe-in-big-brother-watch-v-uk/; N Loideain, 'Not So Grand: The Big Brother Watch ECtHR Grand Chamber judgment' (29 May 2021) Information Law and Policy Centre at https://infolawcentre.blogs.sas.ac.uk/2021/05/28/not-so-grand-the-big-brother-watch-ecthr-grand-chamber-judgment/.

doing so were found fully compliant with Article 6. Article 13 arose for consideration because two of the three applicants had not raised their complaints with the IPT, instead applying directly to the Court. The government argued that those parties had not exhausted all available domestic remedies and, therefore, their complaints were inadmissible under Article 35 § 1 of the Convention. Admissibility turned on whether or not the Tribunal is capable of providing an effective remedy to complainants challenging the overarching compatibility of domestic law with the Convention. The Court found that it is:

> 'as a general rule the IPT has shown itself to be a remedy, available in theory and practice, which is capable of offering redress to applicants complaining of both specific incidences of surveillance and the general Convention compliance of surveillance regimes.'[3]

Nonetheless, the applications were deemed admissible because at the time of application the parties had relied on *Kennedy v United Kingdom*,[4] in which the Court had held that the IPT was not an effective remedy with respect to general complaints about domestic law. The complaint under Article 6 alleged that the IPT was biased and procedurally unfair, for reasons discussed in detail below. That complaint was dismissed as ill-founded for broadly the same reasons that the IPT was held to be an effective remedy for the purposes of Article 13.[5]

Crucial to the Court's endorsement of the IPT was the identification and endorsement in the judgment of what is referred to as the 'elucidatory function'. This refers to a process that first emerged when issues arising from the Snowden disclosures came before the IPT. During those cases, the Tribunal went into closed session with the government's lawyers and a specially

---

[3] n 1 above, at [265]; for full analysis see [250]-[265].

[4] *Kennedy v United Kingdom* [2008] ECHR 1575, [2011] 52 EHRR 4.

[5] n 1 above, at [510].

appointed Counsel to the Tribunal, excluding the public and the complainants. After reviewing classified rules and guidance concerning surveillance programmes, it made details of those rules known to the public with the consent of the government. The First Chamber found that,

> 'the IPT, as the only tribunal with jurisdiction to obtain and review 'below the waterline' material, is not only the sole body capable of elucidating the general operation of a surveillance regime; it is also the sole body capable of determining whether that regime requires further elucidation… the Court considers that the IPT can – and regularly does – elucidate the general operation of surveillance regimes, including in cases where such elucidation is considered necessary to ensure the regime's Convention compliance.'[6]

This article explores the elucidatory function and the normative weight attached to it. It shows that it arose not by design, but as the outcome of an iterative series of procedural innovations through which the Tribunal adapted to unexpected contingencies at the interface between national security and the public sphere, where the Tribunal faces competing imperatives: a risk-based imperative to protect the secrecy of surveillance techniques and a legal imperative to let the public know the law. As the former Independent Reviewer of Terrorism Legislation David Anderson QC put it, public-facing independent review presents difficult challenges to the law where 'potential conflicts between state power and civil liberties are acute, suspicion rife and yet information tightly rationed'.[7] There are similar institutions facing this challenge, as a recent critical review of the UK's accountability mechanisms in respect of national security shows.[8]

---

[6] n 1 above at [255], [257].

[7] D Anderson, 'A Question of Trust: Report of the Investigatory Powers Review' (Independent Reviewer of Terrorism Legislation, 2015) at https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf, [246].

[8] L Woods OBE, L McNamara, J Townend, 'Executive Accountability and National Security', (22 February 2021) Modern Law Review Early Access doi.org/10.1111/1468-2230.12624.

The substance of the IPT's findings on the Snowden disclosures have been subject to criticism elsewhere.[9] This article takes the opportunity to look closely at its procedures, where the unpredictable interaction of judicial process and national security can provoke change and adaptations. It outlines four stages in the development of the Tribunal. First, the period prior to the introduction of legislation on surveillance powers in Britain; second, the period between 1985 – 2000, when a tightly controlled secret judicial body was in operation; third, the development of the contemporary Tribunal that hybridised openness and closure; and finally, the emergence of the elucidatory function.

Contingency and evolution

The analysis presented below is premised on social systems theory. The theory aims to provide a framework capable of describing and analysing the complex and functionally differentiated systems of society – law, science, economics, media, religion, politics, and so on – and the ways that these different systems 'irritate' one another. A full exposition of the theory's often counter-intuitive abstractions is not provided here, but some key concepts must be briefly outlined.[10]

Systems theory supposes that society is composed only of communication. Everything else – notoriously including human bodies and minds – is in communication's environment, which communication observes and communicates about. Modernity is defined by multiple functional systems of communication that have, over time, differentiated themselves from one another and

---

[9] M H Murphy, 'Transparency and Surveillance: assessing the approach of the Investigatory Powers Tribunal' (2016) Public Law 9, K Hughes at n 2 above.

[10] A good introduction is N Luhmann, *Social Systems* (tr. J Bednarz, Jr. with D Baecker, Stanford: Stanford University Press, 1995).

are generative of meaningful communication, each according to its own unique binary 'code'. The legal system utilizes the code of legal/illegal.

Each system defines for itself its own boundary with its environment, which is to say, in the physical environment or, more commonly, in other systems. System/environment is a distinction which is recursively reiterated within a system with each communicative operation. The distinctions drawn by the system allow it to observe *what* is in its environment and, at the second-order level, they allow it to observe *how* it observed its own previous observations. Systems are self-reproducing, using the results of previous operations as the basis and precondition for further operations, each of which redraws the boundary between system and environment. The environment is not a universal constant but a horizon of complex signals that are apprehended by the system according to its own selection criteria. In this sense, systems operate autopoietically.

Functional differentiation presupposes systems are operatively closed as a condition of being cognitively open: the legal system can only communicate using legal communication. If a topic of communication cannot be coded according to legal/illegal, it remains in the environment of the system. As a simple demonstration, consider that a court communicating about a case using another system's media of communication – for instance, deciding for the litigant who offers to pay more money, or the side favoured by the ruling party – would be considered corruption.

A methodological advantage of systems theory's abstraction is to allow an observer to observe how systems use self-produced observations to reflexively alter their own operations. Observers must therefore take systems on their own terms and not account for their observations by reference to unidimensional causes such as 'social forces', 'ideology', or 'economic utility', and so on. Political or economic analyses of law equate to observing one system's observations at the second-order level using the code of another system. Yet, for Luhmann, that is the condition of

modern society: it is nothing other than the second-order observations of observers. Although it may initially appear dogmatic, there is nothing predictive about the theory. Radically decentred, it presupposes contingency, process, and emergence over substance, for there is no Archimedean point or *prima causa* from which society can be explained.[11]

For Luhmann, law's function in modern society is to produce normative expectations about the future, meaning communication about consistent and stable expectations about what ought to happen. Legal expectations are counter-factual, remaining stable even when one experiences cognitive disappointment as events transpire. If, for instance, a government violates human rights law, one may be unsurprised, but can nevertheless seek resolution in the legal system. It is an evolutionary achievement that law remains stable even though what is legal and illegal frequently changes in response to contingencies.[12] Changes in the law may derive from internal or environmental factors: the 'irritations' caused by political events, scientific developments, economic changes, and so on. Such changes occur through recognised procedural programmes – primarily judicial decisions and legislative changes. Legal practitioners and academic observers are rarely concerned with either the code of law or its sociological function, which are taken for granted, but do pay attention to the 'programmes' of the system – legally valid procedures for observing facts in the environment of the system and applying the code in any given case. Change is evolutionary. Systems evolve through adapting their own operations to accommodate contingent events that occur in their environment. Evolution comprises three components. First, an event contingently gives rise to the potential for making a variation from past structures; next,

[11] A Pottage, 'Power as an Art of Contingency: Luhmann, Deleuze, Foucault' (1998) 27 Economy and Society 1, 1.

[12] N Luhmann, *Law as a Social System* (tr. K Ziegert, Oxford: Oxford University Press, 2004) 147-156.

rather than repeating past selections, a variation is selected; finally, the variant selection is restabilized and becomes part of the self-reproduction of the system.[13]

When considering law and official secrecy, an account of publicity is necessary, which in turn requires a systemic account of mass media. The system of the mass media is irreducible to institutions or technical media. It is the system of communication that structures modern society's communication about itself. In Luhmann's analysis, it operates according to the binary code of information and non-information. The mass media's code of information/non-information constantly reacts to its own outputs. Topics are selected as news (information) and, in the process, become non-information. The same information cannot be news twice. Information (surprise) is constantly transformed into redundancy (memory) as soon as it is published. In this way the mass media system forces itself to constantly produce new information. This account of the mass media provides a unique account of the structure of 'common' knowledge in society.[14] For Luhmann, the general symbol of mass media is 'public opinion', which is "the medium of self- and world description of the modern world".[15] In this way, mass media structure the environments of other social systems, provoking communication about new topics, and providing the option to communicate – or not – with 'the public'.

The story that follows concerns evolutionary change at the interface between systems. In one dimension it concerns law and politics, as does all public law, while in another dimension it concerns the interface between law and mass media.

---

[13] ibid 232.

[14] N Luhmann, *The Reality of the Mass Media* (tr. Kathleen Cross, Cambridge: Polity Press, 2000), 20-21, 66; N Luhmann *Theory of Society* (vol.2) (tr. Rhodes Barrett, Stanford: Stanford University Press, 2013) 318-322.

[15] N Luhmann, *Theory of Society* (vol.2), ibid 322.

Stage one: the need to decide.

In 1979 the case of *Malone v Metropolitan Police Commissioner* came before the High Court.[16] Malone was an antiques dealer who was tried for handling stolen property before the Crown Court. During the trial his barrister asked to see a police officer's notebook. It contained a cryptic reference to information that could only have derived from a telephone wiretap.[17] The police admitted there had been interception carried out on the authority of a warrant from the Secretary of State. Malone alleged that the tapping had been ongoing for some time and that he had otherwise been harassed by the police. He sought relief from the High Court, where the Solicitor General intervened on behalf of the Home Secretary.

The case is known to students of public law for the controversial finding in the judgment by Mr Justice Megarry, Vice Chancellor, and Privy Councillor, that the Crown is free to act as if it were an individual. Like anyone else, the Crown may do whatever is not expressly prohibited, requiring no positive legal grounds to authorise action, provided that action does not infringe anyone's rights. This followed the dismissal of arguments that Malone's rights had been violated by tapping; arguments based on property, privacy, and confidentiality.[18] His final argument concerned the principle of legality. As the Vice Chancellor put it,

> 'The underlying assumption of this contention, of course, is that nothing is lawful that is not positively authorised by law. As I have indicated, England is not a country where everything is forbidden except what is expressly permitted…

[16] *Malone v Metropolitan Police Commissioner* [1979] Ch 344.

[17] The facts as recounted in Parliament, HC Deb 12 March 1985 vol 75, col 238.

[18] J Lambert, 'Executive Authority to Tap Telephones', (1980) 43 Modern Law Review 59 provided a comprehensive contemporary case note.

> [telephone tapping] can be lawfully done simply because there is nothing to make it unlawful.'[19]

Students of public law may recall that in 1984 the ECtHR found that the lack of a positive legal basis for such powers meant that the UK had violated the Convention.[20] This precipitated the UK's first legislation on the interception of communications in the form of the Interception of Communications Act 1985.

Aspects of the procedure adopted by the High Court are worth recounting. Malone initially sought an interlocutory injunction to prevent further tapping, and orders for the delivery up of recordings, the destruction of all material held by the police, and damages.[21] He also issued a subpoena to the Post Office for production of the warrant.[22] An employee of the Post Office attended court with a copy of the warrant, which 'lay, like some sacred scroll, untouched upon Megarry's bench inside a sealed envelope'.[23] The warrant remained unopened because on day two of the hearing the plaintiff's statement of claim was altered by consent. On the authority of *American Cyanamid Co. v Ethicon Ltd.* [1975] AC 396, the question of law had to be clarified before any interlocutory injunctions could be made. Hence all claims to orders for delivery or destruction of material were abandoned in favour of an application for general declarations on the law; primarily, a statement

---

[19] n 16 above, 366-367.

[20] As expected, ibid 362-366. The case is *Malone v United Kingdom* (1985) 7 EHRR 14.

[21] n 16 above, 348 H.

[22] ibid 351 F

[23] P Fitzgerald and M Leopold, *Stranger on the Line: the Secret History of Phone Tapping* (London: The Bodley Head, 1987) 135.

that interception of telephone calls is unlawful even if done pursuant to a warrant.[24] Consequently, the court declined to enforce the subpoena.[25] As the Vice Chancellor put it,

> 'On all hands anxiety was shown to have the motion decided not on the basis of whether in fact there has been or still is any tapping of the plaintiff's telephone, but on the basis of whether such tapping, if it takes place, is lawful.'[26]

Throughout the eight days of argument on the law, he had serious doubts about whether or not he should have allowed the action to have proceeded on the basis of hypothetical assumptions with no consideration of evidence of the underlying facts. He did so only on the basis of 'my growing suspicion that ultimately my conclusion would be that none of the declarations [of unlawfulness] ought to be granted'; this way, 'I do not think any harm has been done.'[27] He adds that where an application for a declaration rests on factual premises, rather than construction of a document or statute, courts should be reluctant to grant them, particularly where they are general and widely applicable.[28] This is made all the more acute when the facts have been hypothesised.

The judgment is thus a tentative one. Megarry VC emphasises that telephone tapping 'is a subject which cries out for legislation,'[29] and in the final paragraph states that his judgment is purely 'confined to the tapping of the telephone lines of a particular person which is effected by the Post Office on Post Office premises in pursuance of a warrant of the Home Secretary in a case which

---

[24] n 16 above, 350.

[25] ibid 355 E.

[26] ibid 349 H.

[27] ibid 382 F-G.

[28] ibid.

[29] ibid 380 G.

the police have just cause…'[30] Given that this *obiter* exercise in scope limitation contradicts entirely the implication of his ruling on the question of legality, it seems to indicate deep unease.

Nevertheless, when read in functional political terms, the judgment was a useful stopgap measure. It permitted telephone tapping to continue, by suspending factual analysis in favour of law, it kept the material facts of the practice out of the public domain, and it pre-emptively ruled out any further legal challenges to the practice. JAG Griffith wrote that judges are 'part of the machinery of authority within the State… [they] cannot avoid the making of political decisions',[31] and as Peter Goodrich observed of this case, there was 'a certain inevitability to the court's rejection of [the principle of legality] argument; brave would be the contemporary judge who ruled a long-established state practice to be unlawful'.[32]

Thus, a policy of absolute secrecy over the interception of communications – a policy that had lasted centuries – was preserved a little longer. Prior to the *Malone* case, occasional public controversies over the ambiguous legality of the interception of communication had been dealt with politically, and never before the courts.[33] But where politicians and officials can choose to wait for controversy to recede, courts cannot.

> 'Courts have to decide even when they cannot decide… And if they cannot decide, they must force themselves to be able to decide. If the law cannot be

---

[30] ibid 383 H – 384 B.

[31] J A G Griffith, *The Politics of the Judiciary* (Fontana Press: London 1997) 293.

[32] P Goodrich, 'Freedom of the Phone' (1981) 3 Liverpool Law Review 2 91, 93.

[33] See, for instance, *Report of the Committee of Privy Councillors Appointed to Inquire into the Interception of Communications* HC Cmnd 283 (1957); *Report from the Secret Committee on the Post Office* HC (1844), for a contemporary historical review of the law, P Glover, *Protecting National Security: a History of British Communications Investigation Regulation* (Abingdon: Routledge, 2021).

> found, it must simply be invented… the decision must be translated into distinctions which can be managed, for example the distinction between decision and consequence or between legal principle and its application.'[34]

Legally, the judgment in *Malone* assigned an unconvincing, troubling, yet nonetheless plausible place to telephone tapping within the law in response to an unexpected contingent event while preserving the facts of the matter from analysis. Observed another way, it produced political time, a period in which telephone tapping could continue without disruption while the law was changed by way of legislation. To this extent, the case prefigures the elucidatory function.

Stage two: a limited form of independent appeal

The qualified rights of the ECHR place negative obligations on states not to interfere with individuals' enjoyment of those rights, unless it is necessary to do so, and then only in carefully prescribed circumstances. Measures that interfere with rights must first be 'in accordance with the law' for the purposes of Article 8(2), or 'prescribed by law' for purposes of Articles 9(2), 10(2) and 11(2). This not only means there must be some basis in domestic law for the measure, but that the law has the qualities of accessibility and foreseeability, as elaborated in *Sunday Times v United Kingdom*:

> 'Firstly, the law must be adequately accessible: the citizen must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case. Secondly, a norm cannot be regarded as a "law" unless it is formulated with sufficient precision to enable the citizen to regulate his conduct: he must be able - if need be with appropriate advice - to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail. Those consequences need not be foreseeable with absolute certainty: experience shows this to be unattainable.'[35]

---

[34] n 12 above, 289.

[35] *Sunday Times v United Kingdom* (1979) EHRR 245 at [49].

In *Malone v United Kingdom*,[36] the Court held that the practical need for secrecy in the exercise of surveillance powers inevitably limits the degree of foreseeability that the law must provide:

> '[..] the requirement of foreseeability cannot mean that an individual should be enabled to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly. Nevertheless, the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence. […] the detailed procedures and conditions to be observed do not necessarily have to be contained in the substantive law itself.'[37]

The Court found that in the UK, 'the minimum degree of legal protection to which citizens are entitled under the rule of law in a democratic society is lacking.'[38] Citizens had no way of knowing whether they could be lawfully targeted, and Article 8(2) was violated.

The same principles have been reiterated in subsequent cases in which the Court has been required to consider the compatibility of domestic laws, or the absence of law, governing secretive powers with the Convention. The tension remains fundamentally the same. On one hand governments seek to limit the risk of publicising operational powers that are exercised in secret. On the other hand, the law demands that there must be law in place to limit the potential for arbitrary abuses of secret powers in ways that undermine democracy and human rights, and moreover, it demands that citizens be able to identify these laws in order to foresee the circumstances under which such powers might be used against them, and to know what safeguards exist to limit what use might be

---

[36] n 20 above.

[37] ibid at [67]-[68].

[38] ibid at [79].

made of their private communications if intercepted.[39] Foreseeability does not extend to knowing that the authorities are in fact likely to intercept their communications, as that would allow targets to adapt accordingly, only that citizens can form stable normative expectations in general terms. In systems theoretical terms, it is a reflexive norm: a rule that requires rules be publicly accessible. The legal system regards itself as a communicative medium that can stabilise future expectations in the face of unknowable contingencies that secret surveillance powers create. In its supervisory role, the ECtHR has often performed the second-order role of assessing the quality of the information that the law communicates. It is worth noting that in cases where states are found to have infringed on qualified Convention rights in a manner 'not in accordance with the law', that finding is itself deemed just satisfaction.[40] Insofar as no damages are awarded to the complainant, a finding of 'not in accordance with the law' indicates a failure of the state with no specific victim.

The *Malone* case followed the controversial 'ABC trial' of 1978,[41] where three co-defendants were charged with offences under the Official Secrets Act 1911 in relation to a 1976 *Time Out* report, 'The Eavesdroppers', documenting the activities of GCHQ. This included details of 'Tinkerbell', an advanced centralised tapping installation for conducting electronic domestic surveillance.[42] After *Malone*, the political decision to legislate could no longer be deferred. The state's peremptory response was a 1980 White Paper that led to a review by Lord Diplock of existing interception

---

[39] See for instance *Roman Zakharov v Russia* (2016) 63 EHRR 17 at [229]; n 1 above, at [305]-[310].

[40] See for instance n 20 above, n 35 above, n 39 above.

[41] *R v Aubrey, Berry and Campbell* (1978, unreported); see also Glover at n 33 above, 102.

[42] D Campbell, 'My Life Unmasking British Eavesdroppers' (3 August 2015) *The Intercept* at https://theintercept.com/2015/08/03/life-unmasking-british-eavesdroppers/ ; D Campbell and M Hosenball, 'The Eavesdroppers' (May 1976) *Time Out* at https://www.duncancampbell.org/menu/journalism/timeout/Eavesdroppers.pdf.

practices.[43] As Goodrich noted in his contemporary critique, the Diplock review was thin, avoided reference to the factual controversies that precipitated it, reported that everything was in good order, and silently excluded Northern Ireland from consideration, where large parts of the population were living under constant military surveillance.[44]

Malone's victory in Strasbourg came as no surprise to the government, which had quietly taken a proactive approach to the question of legislation. In March 1979, the Home Office convened a secret Working Party to plan legislation. The Working Party anticipated that the ECtHR would insist that the UK needed to make legislation, and therefore, decided that such legislation:

> 'would be best framed in such a way as to avoid cases becoming justiciable as a result. Our legal advice is that this cannot be done with certainty… In order to provide a limited form of independent appeal, we also recommend the appointment of three advisers to the Secretary of State to whom aggrieved persons could appeal. These advisers would have access to the files on the case in question. They would not be able to tell the individual whether or not his telephone had been tapped; but they would be able to assure him that if it had been tapped this had been done for good reason and the proper procedures followed.'[45]

From a political perspective, the subsequent Interception of Communications Act 1985 (IOCA) primarily served to protect the security of the system. A sparse piece of legislation, it contains twelve sections and two schedules. Section 2 empowered the Secretary of State to issue interception warrants in the interests of national security, for preventing or detecting serious crime, or, where it concerned overseas communications, for the purpose of safeguarding the 'economic

---

[43] *The Interception of Communications in Great Britain*, Report Cm 8191 (1981).

[44] n 33 above.

[45] Interception of Postal and Telephone Communications: Interception Working Party Correspondence (1979) National Archives HO 325/536.

well-being of the United Kingdom'. Section 3 defined the scope of interception warrants. Warrants under section 3(1) required that the targeted person or premises be identified. Warrants under section 3(2) did not, but only applied where a warrant was aimed at 'external communications' intercepted in transmission by a 'public telecommunication system'. For each section 3(2) warrant a certificate was to be issued describing the intercepted material sought. Such a certificate could not be used to specify an address within the UK, unless the examination of communications to or from that address were deemed necessary 'for the purpose of preventing or detecting acts of terrorism'. In other words, IOCA created targeted interception powers for domestic interception and bulk interception powers for intercepting overseas communications. Bulk interception of communication was permitted within the UK only if it concerned terrorism, an exception that was most likely drafted with Northern Ireland in mind.

Safeguards for the handling of intercepted data were created under section 6, while section 7 created the Interception of Communications Tribunal (ICT). An ouster clause stated that the decisions of the ICT were not to be subject to review or appeal by any court.[46] No information disclosed to the Tribunal was to be provided to any other person, unless authorised by its source, and the Tribunal was not to provide reasons for its decisions.[47] The Tribunal was empowered to 'determine their own procedure'.[48] Section 9 IOCA excluded interception evidence from use in court, banning all evidence or cross examination that might suggest interception was taking place by a state authority, lawful or otherwise. This ensured that the blunder made by the police in the Malone trial would not be repeated.

---

[46] Interception of Communications Act 1985 (IOCA) s 7(8).

[47] ibid, Sched 1(4)(2).

[48] ibid, Sched 1(4)(3).

The intended effect of the rules was clear to those paying attention. According to Liberal Democrat MP Alex Carlile,

> 'The powers of the tribunal are virtually purely procedural… It is unlikely, having regard to the nature of the tribunal, that it will provide rules which conform to the rules of natural justice. Indeed, the essence of the secrecy which underpins the tribunal is that it will have to defy the rules of natural justice.'[49]

The ICT was a hermetically closed system, its decisions publicly accessible only in statistical form via the annual reports of the Interception of Communications Commissioner.[50] In the 1997 consultation document that introduced the reforms of the Regulation of Investigatory Powers Act 2000 (RIPA) the Commissioner reported that between its establishment in 1986 and the end of 1997, the ICT had considered five hundred and sixty-eight complaints. In only eight of those cases was interception actually carried out by a government agency. In each case it was authorised by a valid warrant. No complaint to the Tribunal had ever been upheld.[51] The system worked perfectly.

Stage three: procedural autonomy

Between IOCA and RIPA the basic operational distinction between the roles of Commissioner and Tribunal remained the same; the Commissioner acts on an *ex-ante* basis, reviewing ongoing operations and conducting audits of the relevant services to ensure that the law is correctly implemented, while the Tribunal deals with specific *post facto* complaints about the unlawful use of the powers from individuals and organisations. RIPA's enactment was directly linked to the enactment in 2000 of the Human Rights Act 1998, and the main purpose of RIPA, according to its preamble, was to ensure that investigatory powers are 'used in accordance with human rights'.

---

[49] HC Deb 12 March 1985 vol 75, col 238.

[50] The Commissioner's role took on a statutory basis under s 9 IOCA.

[51] *Interception of Communications in the United Kingdom: A consultation paper*, Cm 4368 (1999).

This is reflected in the jurisdiction of the Investigatory Powers Tribunal, found at section 65(2) RIPA:

> (2) The jurisdiction of the tribunal shall be –
>
> (a) to be the only appropriate tribunal for the purposes of section 7 of the Human Rights Act 1998 in relation to any proceedings under subsection (1)(a) of that section (proceedings for actions incompatible with Convention rights) which fall within subsection (3) of this section.
>
> (b) to consider and determine any complaints made to them which, in accordance with subsection (4), are complaints for which the tribunal is the appropriate forum.
>
> (c) to consider and determine any reference to them by any person that he has suffered detriment as a consequence of any prohibition or restriction, by virtue of section 17, on his relying in, or for the purposes of, any civil proceedings on any matter; and
>
> (d) to hear and determine any other such proceedings falling within subsection (3) as may be allocated to them in accordance with provision made by the Secretary of State by order.

When the IPT receives a complaint that falls within its jurisdiction, it is to discover first whether the alleged acts have occurred, and where so, it is to examine the purported authority for those acts, applying judicial review principles.[52] Like the ICT, determinations were intended to be final, with section 67(8) intended to function as an ouster clause. However, in *R (Privacy International) v Investigatory Powers Tribunal* that clause was held ineffective by the Supreme Court.[53]

---

[52] RIPA s 67(2) and s 67 (3)(c).

[53] *R (Privacy International) v Investigatory Powers Tribunal* [2019] UKSC 22. For insightful commentary, Paul F Scott, 'Once More unto the Breach: *R (Privacy International) v Investigatory Powers Tribunal)* (2020) 24 Edinburgh Law Review 1 103. Section 242 of the Investigatory Powers Act 2016 (IPA) has amended RIPA by adding a new section 67A,

The IPT's panels are empowered 'to determine their own procedure in relation to any proceedings'[54] subject to procedural rules made by the Secretary of State.[55] A complaint can be finally determined in one of two ways: the IPT can either make a determination in favour of the complainant, or make a statement that no determination has been made in the complainant's favour.[56] If a complaint is upheld, a report must be made to the Prime Minister explaining the finding.[57] Where it is not, the mandatory response that no determination has been made in the complainant's favour is intentionally ambiguous. The complainant cannot discover whether they are under lawful surveillance or are not under surveillance at all. This intentionally mirrors the official government policy of 'neither confirm nor deny', or NCND, a position of deliberate ambiguity in response to questions concerning operational surveillance matters and other areas of official secrecy designed to minimise the risk that hostile actors could piece together seemingly innocuous information to build a 'mosaic' of intelligence.[58]

Despite being legislatively structured like the ICT, the IPT began evolving almost immediately. In 2002, two parties, joined by the *Guardian* newspaper, challenged the procedural rules laid down by

---

which provides for a right of appeal to the Court of Appeal or Court of Sessions against certain decisions of the Tribunal on a point of law.

[54] Regulation of Investigatory Powers Act 2000 (RIPA) s 68(1).

[55] ibid s 69.

[56] ibid s 68(4). Vexatious or frivolous are dismissed under s 69.

[57] ibid s 68(5).

[58] The non-transparency of this policy has been criticised by civil liberties campaigners. See, 'To "Neither Confirm Nor Deny": Assessing the Response and its Impact on Access to Justice' (2017) JUSTICE at https://justice.org.uk/wp-content/uploads/2018/02/NCND-Brochure_FINAL_WEB_Spreads2.pdf.

the Secretary of State on grounds of incompatibility with Articles 6, 8 and 10 of the Convention.[59] The first complainant was an individual named Kennedy who had alleged that the police had placed him under unlawful surveillance.[60] The second was a group of three NGOs, Liberty, British Irish Rights Watch, and the Irish Council for Civil Liberties. They challenged the legality of the UK's interception of a microwave link carrying most of Ireland's telecommunications traffic at a Ministry of Defence facility in Capenhurst, Cheshire,[61] from 2 October 2000 onwards – the date the Human Rights Act 1998 came into force.[62] They had previously and unsuccessfully challenged the same system before the ICT in September 1999 and had made an outstanding application to the ECtHR. The ECtHR adjourned the matter until the IPT proceedings had concluded. It was eventually decided in 2008.[63]

Oral argument was heard in private in accordance with Rule 9(6) over three days in July and August 2002. The Tribunal then convened in public for the first time on 23rd January 2003 to give judgment in the applicants' favour, finding that Rule 9(6) was *ultra vires* section 69 RIPA and does not bind the Tribunal. It is notable that this finding was based not upon the Convention but on common law. There was, the Tribunal found,

> 'no conceivable ground for requiring legal arguments on pure points of procedural law, arising on the interpretation and validity of the Rules, to be heard in private… purely legal arguments, conducted for the sole purpose of

---

[59] The right to a fair trial, the right to respect for family and privacy life, and the right to freedom of expression respectively.

[60] *Kennedy v Security Services, GCHQ and the Met* [2004] UKIPTrib 01 – 62 – 3.

[61] D Campbell and P Lashmar, 'How Britain eavesdropped on Dublin' (15th July 1999) *The Independent* at https://www.independent.co.uk/news/how-britain-eavesdropped-on-dublin-1106606.html.

[62] *British Irish Rights Watch and others v Security Service, GCHQ and the SIS* [2004] IPT/01/77.

[63] *Liberty v United Kingdom* (2009) 48 EHRR 1.

> ascertaining what is the law and not involving the risk of disclosure of any sensitive information, should be heard in public. The public, as well as the parties, has a right to know that there is a dispute about the interpretation and validity of the relevant law and what the rival legal contentions are.'[64]

In all other respects the Tribunal held its own rules and procedures to be lawful.

The Tribunal noted that its ruling was a development 'which may well not have been foreseen when the Rules were made',[65] and there are hints that internal discussions had taken place before the judgment finally appeared. The five-month delay between hearing and judgment was explained as follows:

> 'The responsibility of the Tribunal is a particularly anxious one. It is not within the competence of many courts and tribunals, short of the House of Lords, to make rulings on questions of law apparently unappealable to, and unreviewable by, any other judicial body within the jurisdiction […] The consequent delay… is regrettable, but it was unavoidable while the procedural issues, which are significant for the future conduct of proceedings before the Tribunal, were being resolved.'[66]

For this reason, the judgment regarded itself as contingent, 'subject to re-consideration and revision in the light of increases in the experience of the Tribunal, new developments and fresh arguments.'[67] Nevertheless, it continued, and today the Tribunal's website calls the judgment a 'defining ruling in the early history of the IPT'.[68] The Tribunal had varied its own 'programming'

---

[64] *Kennedy and Other ruling of the Tribunal on Preliminary Issues of Law* [2003] IPT/01/62 & 77, 70-71.

[65] ibid 70.

[66] ibid 7-8.

[67] ibid 7.

[68] This statement only appears on the IPT webpage hosting the judgment, see 'Rulings of the Tribunal on Preliminary Issues of Law' at www.ipt-uk.com/judgments.asp?id=1.

around the distinction between facts and norms: the latter could be argued in public, the former must remain secret.

Thereafter, complaints to the IPT that raised a preliminary question of law were dealt with in open hearings. In such cases, the government maintained a formal stance of neither confirming nor denying the facts. Instead, analysis of the law proceeded on the basis of hypothetical facts: 'if X is the case then…', 'if X is not the case not then…', and the application of the legal findings to the actual facts took place afterwards, in private. Over the following decade, the IPT embraced this practice of hypothecating facts to publicly answer questions of law. The technique of assuming facts which had so troubled Vice Chancellor Megarry in the High Court was much less controversial in the Tribunal, perhaps because the stakes were lower, the questions limited to matters of statutory construction, and because none of the decisions had any legal effect on any person or judicial body other than the Tribunal itself.[69]

A second preliminary hearing was held in the case of *Kennedy* in July 2004 to establish the correct legal approach to his complaints about surveillance that had allegedly occurred prior to the enactment of the Human Rights Act. In its judgment, the Tribunal, citing *Malone*, held there was then no common law right to privacy. The complaint would have to be assessed on the ordinary principles of judicial review, that is, on grounds of irrationality or illegality.[70] In January 2005 the IPT held that no determination had been made in the complainant's favour.[71]

---

[69] See for examples of such rulings *B v Security Service* [2004] IPT/03/01 concerning the validity of the NCND policy in relation to whether an MP had been under surveillance in the 1980s, and *Frank-Steiner v the Data Controller of the Secret Intelligence Service* [2008] IPT/06/81/CH.

[70] n 60 above at [27]-[28].

[71] n 4 above at [20].

Kennedy applied to the ECtHR, arguing that UK's domestic legal regime was incompatible with the Convention. In response, the government argued that his complaint should be ruled inadmissible because he had failed to exhaust his domestic remedies, as required by Article 35 § 1. Unlike the NGOs in the *British-Irish Rights Watch* case, Kennedy had not challenged the lawfulness of the UK's domestic regime in general terms before the IPT. He had complained only about specific alleged violations of his rights. By the time the Court's judgment was issued in October 2010, the IPT had issued twelve public rulings on the law, including those connected to the *Kennedy* and *British-Irish Rights Watch* cases. Most were summaries of upheld complaints against public authorities, while a few clarified the meaning of the law. The government contended that this showed that the Tribunal could adequately assess domestic law, and that before going to the Court, Kennedy ought to have asked the IPT for judgment.

The ECtHR disagreed. It held that it did not matter that Kennedy had not complained to the IPT because, despite the handful of legal questions it had publicly resolved, the Tribunal was incapable of providing adequate redress to general complaints about the domestic legal framework. Put bluntly, the Court had no evidence that the Tribunal's judgments really meant anything. It had no power to strike down or annul any statutory provisions, let alone the power to make a statutory declaration of incompatibility with the Convention under section 4(2) of the Human Rights Act. Even if the IPT were so empowered, the British government had not sufficiently demonstrated that, when faced with a section 4(2) statutory declaration of incompatibility, it would amend the law to remedy the issue and achieve compatibility with the Convention. The Court was not prepared to treat the Tribunal's self-defined role of publicly reviewing domestic legislation as anything more than an academic exercise, and ruled that,

> '… it is unlikely that any further elucidation of the interception regime and applicable safeguards, such as would assist the Court in its consideration of the

> compliance of the regime with the Convention, would result from a general challenge before the IPT.'[72]

Nonetheless, it held that the IPT's procedures for examining an individual's specific complaint are compliant with the right to a fair trial under Article 6, and that the Tribunal constitutes an effective remedy under Article 13 of the Convention. In short, the IPT was approved for handling individual complaints, but not for reviewing the domestic framework.

In its second preliminary judgment in the *British-Irish Rights Watch* case, the Tribunal addressed the accessibility and foreseeability of the law concerning the filtering process that would be applied to intercepted 'external' telephone calls, collected under thematic warrants made pursuant to section 8(4) RIPA. The complainants argued that section 8(4) was insufficiently clear about the rules governing how external communications, intercepted in bulk, would be filtered and selected for examination. They argued that, in order to meet the requirements of foreseeability, 'something more should be said, by way of indication as to selection criteria than is presently stated, and that the selection should not be left simply to the discretion of officials.'[73] But the IPT held existing provisions to be 'sufficiently accessible and foreseeable to be *in accordance with the law*'.[74] The matter then proceeded before the ECtHR.

As the complaint was lodged in 1999 and complained of interception that allegedly occurred between 1990 and 1997, the ECtHR reviewed the regime applicable at the time – IOCA. It found

---

[72] ibid at [110].

[73] n 62 above, at [32.2].

[74] ibid at [39], emphasis original. This finding was reversed by the First Chamber's 2018 ruling in *Big Brother Watch* as explained above.

that the thin description of the warrant regime under section 3(2) was insufficiently accessible and its effects unforeseeable:

> '… the Court does not consider that the domestic law at the relevant time indicated with sufficient clarity, so as to provide adequate protection against abuse of power, the scope or manner of exercise of the very wide discretion conferred on the State to intercept and examine external communications. In particular, it did not, as required by the Court's case-law, set out in a form accessible to the public any indication of the procedure to be followed for selecting for examination, sharing, storing and destroying intercepted material.'[75]

By then, IOCA was repealed and RIPA, containing much more detail about the regime including in its attendant Codes of Practice, was in force. Also, by then, the leading ECtHR case on foreseeability requirements of law governing secret surveillance measures was *Weber and Saravia*.[76] The applicants had complained that German 'strategic surveillance' (what is now referred to as 'bulk' surveillance) of international communications violated their rights under Articles 8 and 10 of the Convention. The Court ultimately held that the complaints were inadmissible because they were manifestly ill-founded, but it set out the following minimum safeguards that legislation on such matters must specify:

> '… the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed.'[77]

These criteria played an important role in the later development of the elucidatory function.

---

[75] n 63 above, at [69].

[76] *Weber and Saravia v Germany* (2008) 46 EHRR SE5.

[77] ibid at [95].

Stage four: elucidation

In the First Chamber judgment in *Big Brother Watch v UK*, two IPT cases are explicitly referred to as evidence of the 'elucidatory function' at work in rectifying defects in the law.[78] They are *Belhadj*[79] and *Liberty v GCHQ and others*.[80] Both complaints were lodged in the aftermath of the Snowden revelations. In both cases the Tribunal identified in interim public rulings flaws in the accessibility and foreseeability of the UK's domestic legal regime. But rather than declaring the government in violation of the Convention, it adapted its own proceedings to actively remedy the flaws.

Belhaj

The *Belhadj* case was satellite litigation derived from the complainant's then-ongoing claim against British officials, notably the former Foreign Secretary Jack Straw and the former head of MI6 counterterrorism, Sir Mark Allen. Mr Belhaj is a Libyan national who was a dissident from the Gaddafi regime. During the revolution that began in Libya in February 2011, Belhaj obtained documentary evidence that in 2004 British officials, alongside US and Libyan counterparts, had arranged for his arrest, detention, mistreatment and extraordinary rendition to Libya, along with that of his then-pregnant wife. He was then imprisoned until 2010. Other victims of British complicity in extraordinary rendition during the so-called 'War on Terror' settled their claims in exchange for compensation, on the condition that the government would not admit fault, but Mr Belhaj and his wife pressed their claim, seeking nominal damages and a public apology from those they alleged were responsible.[81]

---

[78] n 1 above, at [240].

[79] *Belhadj v Security Service,* [2015] 4 WLUK 62, [2014] IPT/13/132-9/H. Mr Belhaj's name was mis-spelled by the Tribunal.

[80] *Liberty v GGHQ* [2015] 3 All E.R. 212, [2015] 2 WLUK 215. This report is specifically the open judgment on the law of February 2015 and not the final determination of the complaint.

[81] See Paul F. Scott, *The National Security Constitution* (Hart, 2018) 253-258.

At the time of the Snowden revelations in mid-2013 his claim was before the High Court, where the government challenged it on grounds of non-justiciability.[82] In September 2013 Mr Belhaj, his wife, and other Libyan claimants who had settled for compensation in 2012, lodged a complaint with the IPT. Given that they were likely to have been of interest to the intelligence agencies as members or former members of the Libyan Islamic Fighting Group, they submitted that there was a strong likelihood that privileged communications with their lawyers would have been intercepted. They argued on the basis of *Steidl v Enyo Law* [2011] EWCH 2649 (Comm) that there was a common law and equitable principle that no lawyer or official who had reviewed any intercepted legally privileged communications could be permitted to act in the government's defence of the civil claim before the High Court, and sought an injunction to protect their legally privileged communications from being passed to the government's legal team accordingly.

The government gave an interim undertaking that no such lawyer or official would have sight of any such material, the existence of which was subject to NCND, and this was accepted by the Tribunal in its first preliminary judgment in January 2014.[83] A second judgment was handed down in November 2014,[84] the substantive legal question in the case defined as follows:

> 'On the hypothetical assumption (the true position being neither confirmed nor denied) that the Claimants' legally privileged materials have been intercepted by the Respondents and/or have been obtained by the Respondents as part of their intelligence sharing regime:

---

[82] *Belhaj v Straw* [2013] EWHC 4111 (QB); the Supreme Court found it was justiciable, *Belhaj v Straw* [2017] UKSC 3.

[83] n 79 above.

[84] This interim decision was handed down on 18th November 2014. It is not included in the report on the final determination of the Tribunal at n 79 above but has the Tribunal citation IPT/13/132-9/H and is available at https://www.ipt-uk.com/judgments.asp?id=22.

> 1. Is the regime for the interception/obtaining, analysis, use, disclosure and destruction of legally privileged material prescribed by law for the purposes of Article 8(2) of the ECHR?
>
> 2. Has this been the case since January 2010?'[85]

Before the second hearing, the government served two documents on the claimants: an 'open' Response addressing the legal and policy regime on the question of how legally privileged material is handled if it is intercepted, and a summary of the 'closed' Response. The 'closed response' was served only on the Tribunal. It was said to contain details of a classified regime of rules regarding intercepted privileged material. The government claimed that its disclosure would be contrary to the public interest.

The claimants were not satisfied with a mere summary. They argued that, on the best evidence rule,[86] the Tribunal should at least order the government to serve full copies of the classified documents, redacted where necessary, rather than a typed summary of their content. The Tribunal rejected this submission on the basis that,

> 'The purpose of the Respondents providing information is to establish the precedent facts, as to the legal and policy regime operated during the material time by the Respondents in relation to legally privileged material. The disclosure is not required, as in general civil litigation, to enable a party to pursue a train of enquiry, assess the authenticity of a document or as the basis for cross-examination.'[87]

---

[85] ibid at [2].

[86] As articulated by Sedley LJ in *R (National Association of Health Stores v Department of Health* [2005] EWCA Civ 154 at [49].

[87] n 84 above, at [9].

Moreover, the Tribunal continued, *it* would not be relying on a second-hand summary. In closed session it 'has the power to inspect the original document, if and when required, to ensure accuracy and authenticity'.[88] The Tribunal rejected the argument that anything relevant to the case could be gleaned from allowing the complainants to assess the form and scale of redactions made to documents as those were facts, whereas the purpose – and indeed the limitation – of an open hearing before the IPT is to answer a question of law.[89] Nevertheless, the Tribunal did make public one factual finding about the documents:

> 'The Tribunal has inspected the documents in respect of which further disclosure is sought. It is satisfied that the protection of intelligence and security interests does require that disclosure should not be given by way of redacted copies of documents, but by summary or retyping.'[90]

At that November hearing, a third hearing to determine the substantive legal question was fixed, but by an order of 26th February 2015, the IPT declared that the government had conceded. The government accepted that since 2010, the regime concerning the interception of legally privileged material had been unlawful, contravening Article 8(2) ECHR. On 29th April 2015 the case concluded with a determination.[91] There had been a breach of the rights of one of the complainants in respect of two intercepted documents. Those documents were ordered destroyed. No compensation was awarded. Against the submissions of the government, the finding that the regime had been unlawful was made public. No determination was made in favour of the other complainants.

---

[88] ibid, at [9].

[89] ibid, at [10].

[90] ibid, at [11].

[91] n 79 above.

Intelligence sharing

Why did the government concede? The answer is to be found in the first of three rulings in the second of the post-Snowden cases, *Liberty v GCHQ*.[92] The case saw five human rights NGOs bring a joint complaint under Article 8 and, by extension, Article 10, in respect of two surveillance programmes revealed by Snowden. The first issue concerned intelligence sharing under Prism, a programme operated by the National Security Agency (NSA) of the United States, which gave officials direct access to the servers of most major US internet service providers and platforms. Documents showed GCHQ had access to Prism, as well as access to data derived from an American bulk interception programme (codenamed 'Upstream'). The power to access material intercepted by a foreign government had no obvious footing in public law. The particular risk of arbitrary abuse of this power lay in the possibility that it could be used to circumvent the privacy-protecting procedures and safeguards attendant to section 8(1) RIPA interception warrants: if GCHQ could not show that it was necessary and proportionate to target an individual with a warrant, there was nothing in law to prevent unwarranted surveillance using Prism instead. The second issue concerned RIPA safeguards themselves. The complainants challenged the lawfulness of 'Tempora', GCHQ's programme for bulk interception of internet traffic via undersea cables, authorised via 'external' interception warrants issued under section 8(4) RIPA. Here we address only the Prism issue, as this was the question resolved by the so-called elucidatory function.

Initially the government maintained a stance of NCND in relation to Prism. This was despite public reports on the issue made by the Intelligence and Security Committee of Parliament (ISC) and the Interception of Communications Commissioner's Office (IOCCO), published prior to the

[92] n 80 above.

hearing, which stated that there was no abuse or circumvention of domestic law as alleged.[93] The reason for maintaining NCND was so as not to render the policy nugatory by responding affirmatively to unauthorised disclosures. The case was therefore heard on the somewhat surreal basis of agreed assumed facts, even though everyone paying attention was sure of the underlying reality.[94]

The key question with respect to intelligence sharing was whether or not it was 'in accordance with the law' for the purposes of Article 8(2) ECHR. The government argued that intelligence sharing was already subject to oversight by the IOCCO and the ISC, and that if intelligence were obtained from a system like Prism, it would not be analogous in law to communication intercepted directly by UK authorities. The government, relying on a witness statement from Charles Farr, the Director-General of the Office for Security and Counter Terrorism, submitted that it would be artificial to distinguish between foreign intelligence obtained from a covert human source, foreign intelligence obtained from interception, and foreign intelligence obtained by access to a programme like Prism.[95] The government was legislatively empowered to obtain information by any such means, while the common law's *Padfield* principle prevented it from using such means to circumvent RIPA safeguards. As such, the *Weber* requirements for the accessibility and foreseeability of laws on interception powers should not apply. Obtaining intelligence from allies is a normal part of the general powers of the intelligence services to gather information and is thus

---

[93] 2013 Annual Report of the Interception of Communications Commissioner, HC 1184 (2014), at [6.8.1-5]; Statement on GCHQ's Alleged Interception of Communications under the US PRISM Programme from the Intelligence and Security Committee of Parliament (17th July 2013), unreferenced document, at https://isc.independent.gov.uk/wp-content/uploads/2021/01/20130717_ISC_statement_GCHQ-1.pdf.

[94] *Liberty v GCHQ* [2015] 3 All E.R. 142 | [2014] 12 WLUK 225, at [13]-[15]. Note that this is the interim judgment of December 2014, distinct from the report of the February 2015 judgment at n 80 above.

[95] ibid, at [26].

already regulated by the statutes governing their activities, which include clear statutory duties not to act in contravention of the Convention, as well as a common law duty not to undermine or frustrate the purpose of legislation such as RIPA.[96]

The Tribunal disagreed, finding that more is required of the law by the jurisprudence of the ECtHR, albeit at a 'lesser level' than the *Weber and Savaria* requirements. The 'lesser level' applies because in accessing data obtained by foreign allies, no actual interception is carried out by UK authorities. Yet as UK agencies would still be selecting, processing, analysing, retaining, and deleting whatever data they obtained, some publicly accessible safeguards were required, and any potential interference with privacy must be made foreseeable, for the regime to be in accordance with the law for the purposes of Article 8(2).[97]

Mr Farr's statement had disclosed that strict rules and guidance existed within the intelligence and security services for handling any such material.[98] He said that these 'arrangements' had been reviewed and that the government maintained that they could not be disclosed publicly without undermining national security and the prevention and detection of serious crime.[99] Consequently, the Tribunal decided that full details of those arrangements need not be made public, but ruled that there must be some form of 'signposting' of the rules and arrangements, such that:

---

[96] ibid, at [19]-[21], [30]; the common law authority is *Padfield v Ministry of Agriculture, Fisheries and Food* [1968] AC 997.

[97] ibid, at [36].

[98] ibid, at [37]. The arrangements were made pursuant to section 2 of the Security Service Act 1989 and section 2(a) and section 4(a) of the Intelligence Services Act 1994.

[99] ibid, at [43].

i) 'Appropriate rules or *arrangements* exist and are publicly known and confirmed to exist, with their content sufficiently signposted, such as to give an *adequate indication* of it …

ii) They are subject to proper oversight.'[100]

Resisting disclosure, the government argued that the reports of the Commissioner and the ISC mentioned above had given sufficient publicity to the fact that such arrangements existed, but the IPT disagreed. As things stood, there was no sufficient indication of the arrangements on intelligence sharing practices anywhere in the law.[101]

At this point, notwithstanding the other issues in the case, it would have been consistent with previous practice of the Tribunal to make a ruling that the UK's domestic legal framework was not in accordance with the law in respect of intelligence sharing under Prism, and to privately determine whether the complainants had in fact been victims of unlawful surveillance carried out via such a system. The political consequences would then have played out in the mass media and in Parliament.

Instead, exercising its power to determine its own proceedings under section 68(1) RIPA, the Tribunal arranged a closed hearing with the government's legal team. During that hearing it adopted a procedure based on advice provided by the specially appointed Counsel to the Tribunal, who suggested the Tribunal direct him to adopt an adversarial role, akin to that of a Special Advocate. He would stand in for the complainants' lawyers and this way, press the argument for

[100] ibid, at [41].

[101] ibid, at [44].

disclosure. The Tribunal could then decide upon which aspects of the secret arrangements on intelligence sharing could safely be disclosed from 'below the waterline'.[102]

Explaining this procedural innovation, the IPT outlined its four 'very distinct advantages over both the Commissioner and the ISC' as follows:

i) 'Having the benefit of *inter partes* argument with submissions from Claimants 'who seek to criticise the system'.

ii) Holding public hearings on assumed facts, assertions that would otherwise be subject to NCND and, as such, would not proceed unless the Claimants could show an arguable case.

iii) Having access to 'all secret information' and the ability to assess it in closed hearings, to confirm that the 'arrangements' do indeed exist and are adequate to protect against arbitrary interference with privacy; and

iv) Having the opportunity, 'with the benefit of full argument, to probe fully whether matters disclosed to it in closed hearing… can and should be disclosed in open and thereby publicised'.[103]

The first two points were established practice; the latter two were novel inventions, deployed for the first time in this case. They are a good description of the key techniques of the 'elucidatory function'.

During the closed hearing, the government agreed to make what the Tribunal called 'a Disclosure',[104] amounting to a short text describing the relevant arrangements drafted by counsel

[102] ibid, at [10] and [45].

[103] ibid, at [46].

[104] ibid, at [47].

for the government. The Disclosure consisted initially of two parts. Part 1 contains two subclauses, 1a) and 1b). Part 1a) states that the Intelligence Services may only make a request to the government of another country for unanalysed intercepted communications if there is a relevant RIPA warrant already in place, the foreign assistance is required because the communications cannot be obtained under that warrant, and it is necessary and proportionate to do so. Part b) applies in the alternative situation where there is no RIPA warrant in place. In that situation, the intelligence services may only make a request to a foreign power for intercepted data if making such a request 'does not amount to a deliberate circumvention of RIPA or otherwise contravene the principle established in *Padfield* … and it is necessary and proportionate … [this] would be considered and decided upon by the Secretary of State personally.' There follows a paragraph of definitions of RIPA warrants; either a targeted or bulk warrant can apply. Part 2 states that where communications content or data are received from a foreign government, the material will be subject to the 'same internal rules and safeguards as the same categories of content or data, when they are obtained directly by the Intelligence Services as a result of interception under RIPA.'[105]

The Tribunal then held an open hearing to hear arguments as to the legal effect of the Disclosure. There, the claimants raised objections to the novel procedure the Tribunal had taken, and to the content of the first Disclosure, which led to a second statement of Disclosure. The second Disclosure refers to the fact that the US government had acknowledged that Snowden's disclosures on Prism and the bulk cable interception programme known as Upstream were true, and states that requests may only be made to the US for 'unanalysed intercepted communications (and associated communications data) acquired in this way'. Secondly, it states that requests as described in 1(b) of the first Disclosure – that is, requests made where no equivalent RIPA warrant

[105] ibid.

was in place – would be made only in exceptional circumstances, and that no such requests had occurred as of the date of disclosure.[106]

The claimants challenged the procedure on the basis that the Tribunal was not entitled to look 'below the waterline' to assess the arrangements, even if adequate indication of them had existed 'above the waterline'. They also criticised the substance of the Disclosure, which was described as a 'running document' in the Tribunal's own terms, for its opacity, for not revealing its sources, nor even indicating whether it was a gist or summary of those sources.[107] The Tribunal rejected these objections, as did the ECtHR when they were later raised in the context of the Article 6 challenge in *Big Brother Watch v United Kingdom*.[108] For the Tribunal, and for the Court, the description provided amounted to sufficient 'signposting'.

The first judgment concludes by finding that both the bulk interception regime under section s8(4) and the intelligence sharing regime were in accordance with the law, save for one exceptional point raised by the complainants. The exception concerned the scenario in Part 1(b) of the first Disclosure, i.e., requests not already covered by an equivalent RIPA warrant. The government had stated that such requests would only occur in exceptional cases, and that none had ever occurred. But it remained unclear whether such data would, if ever received, be held subject to the same safeguards that apply to data intercepted by UK authorities under section 16(3) RIPA. The Tribunal invited further representations on that point and adjourned for a further hearing.

---

[106] ibid, at [48].

[107] ibid, at [49].

[108] n 1 above, at [510].

A second judgment in the case was handed down on 6th February 2015.[109] It first addressed whether the Disclosures, which had not been published anywhere other than in the Tribunal's December 2014 judgment, were legally necessary in order for the intelligence sharing regime to be made in accordance with the law under Article 8(2). The government had maintained that they were not necessary because the pre-existing legal framework had been adequate.[110] But the Tribunal explicitly confirmed that the Disclosures were required, and furthermore, that the *IPT itself* had been the medium for their communication to the public:

> 'It is only by reference to the Disclosures that [we were] satisfied that there was a sufficiently accessible indication to the public of the legal framework and any safeguards. In the absence of the Disclosures any such indications would have been insufficient and the intelligence sharing regime would not have been in 'accordance with the law/prescribed by law' […] without the disclosures made, there would not have been *adequate signposting*, as we have found was required and has now, as a result of our Judgment, been given.'[111]

To address the exceptional question from the December judgment, the government issued a third Disclosure, stating,

> '[…] in the event that a request falling within paragraph 1(b) of the Disclosure were to be made and approved by the Secretary of State other than in relation to specific selectors (i.e. "untargeted"), the Intelligence Services would not examine any communications so obtained according to any factors as are mentioned in section 16(2)(a) and (b) of RIPA unless the Secretary of State personally considered and approved the examination of those communications by reference to such factors.'[112]

---

[109] n 80 above.

[110] ibid, at [20].

[111] ibid, at [19] and [21].

[112] ibid, at [30].

The Tribunal held that this was sufficient, and on that basis made the following order:

> '(i) THAT prior to the disclosures made and referred to in the First Judgment and the Second Judgment, the regime governing the soliciting, receiving, storing and transmitting by UK authorities of private communications of individuals located in the UK, which have been obtained by US authorities pursuant to Prism and/or (on the Claimants' case) Upstream, contravened Articles 8 or 10 ECHR, but
>
> (ii) THAT it now complies with the said Articles.'[113]

Final determination of the case followed in June 2015. The Tribunal made no determination in favour of all parties but two – Amnesty International and the Legal Resources Centre in South Africa. Emails associated with those organisations had been intercepted pursuant to bulk interception warrants under section 8(4) RIPA. The interception and examination of these communications were in both cases found to be necessary and proportionate, but in the case of Amnesty an email had been retained by GHCQ for a longer period than lawfully permitted, while in the case of the Legal Resources Centre, the selection process by which the communications were selected for examination did not follow the protocol laid down by GCHQ's internal policies. Neither organisation was held to have suffered any material detriment and no compensation was awarded.[114]

The self-referential aspect of the Tribunal's judgment is unique. To be clear, the text of the judgment itself containing the three-part Disclosure, which is the only published record of that Disclosure, is a critical material factor in the judgment's conclusion on the law. The text is both a legal analysis of the law as a communicative medium, and a critical piece of information that is

---

[113] ibid, at [32].

[114] *Liberty v GCHQ* [2015] 6 WLUK 674.

added by, and included within, that analysis. It is performative in the truest sense: a text that changed the situation it describes. The paradoxical outcome is that a situation which was found to be illegal was made legal by the process that found it.[115] The judgment takes its own date of publication as a key moment in legal time, reflexively converting an unlawful past into a lawful future. In a supposedly adversarial process, both sides won.

Further elucidations

Elucidatory analysis occurred in two further cases arising from Snowden's revelations. They are presented here only to show how the elucidatory function continued to inform the Tribunal's practice. The first concerns 'equipment interference' (EI), also referred to as 'computer network exploitation' (CNE), euphemisms for computer hacking. The second concerns the secret procurement of bulk datasets. Neither of these deeply intrusive powers were clearly prescribed by law in the UK prior to the Snowden revelations.

A complaint that hacking was not in accordance with the law was lodged in May 2014 by Privacy International alongside seven internet service providers.[116] The government responded to all allegations with NCND until 6th February 2015, the day of the Tribunal's self-referential judgment in the *Liberty v GCHQ* case, when the practice was publicly 'avowed' in a consultation document that accompanied the publication of a draft Equipment Interference Code of Practice.[117] As the

---

[115] B Keenan, 'Going 'below the waterline': the paradoxical regulation of secret surveillance in the UK' (2015) LSE Law Policy Briefing Series (9).

[116] *Privacy International v Secretary of State for Foreign and Commonwealth Affairs* [2016] 2 WLUK 351.

[117] Consultation: Equipment Interference and Interception of Communications Codes of Practice (2015) Home Office, at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/401867/Consultation_on_the_draft_Codes_of_Practice_on_Interception_and_Equipmen....pdf; draft Equipment Interference

Tribunal notes in its judgment, this was the same date that the government served their Open Response: clearly the *Liberty* decision had created a 'knock on' effect on the government.[118]

The Tribunal also noted that the government had responded to the litigation by amending the Serious Crime Bill in June 2014, modifying section 10 of the Computer Misuse Act 1990 to expand the scope of exceptions to the offence of unlawfully accessing and modifying a computer system.[119] Certain arrangements 'below the waterline' had entered the public domain 'as a result of the disclosure sought by the Claimants, and by Counsel to the Tribunal, and requested by the Tribunal'.[120] The Tribunal also recorded that it had influenced the findings of the Independent Reviewer of Terrorism Legislation in his June 2015 report to the Prime Minister on the use of bulk investigatory powers, including hacking.[121] For all this, elucidation was not the determinative issue in the case. The IPT held that hacking was in accordance with the law both before and after the avowals of February 2015.

In *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others*,[122] the order of events was unusual in that it began with deliberate government disclosure of previously classified information. In March 2015, a month after the decision in *Liberty/Privacy*, an ISC report

---

Code of Practice (2015) Home Office, at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/401867/Consultation_on_the_draft_Codes_of_Practice_on_Interception_and_Equipmen....pdf.

[118] n 116 above, at [11(i)].

[119] ibid.

[120] ibid, at [11(ii)].

[121] ibid, at [11(iii)]; the report is 'A Question of Trust' at n 7 above.

[122] *Privacy International v Secretary of State for Foreign and Commonwealth Affairs* [2018] 4 All E.R. 275. This was the last in a series of four open judgments on the law, all prior to a final determination.

revealed that the intelligence and security services acquired and used bulk personal datasets (BPD).[123] The BPD included sensitive personal data on millions of individuals, the majority of whom were of no intelligence interest, and was used to build and develop analytic systems aimed at detecting individuals and patterns of interest. The government argued that this was in accordance with the general statutory powers to acquire information granted by the Security Service Act 1989 and the Intelligence Services Act 1994.[124] On 4th November 2015, as the draft Investigatory Powers Bill was presented to Parliament, the government disclosed that it had obtained bulk communications datasets (BCD) from communication service providers by issuing them with directions pursuant to section 94 of the Telecommunications Act 1984.[125] Handling arrangements in respect of both BPD and BCD were published on the same day.

The Tribunal assessed the legality of the practices before and after these avowals. As no rules existed in the public domain about the acquisition and use of bulk datasets, the Tribunal concluded in its first judgement in October 2016 that both regimes had not been in accordance with the law prior to March 2015 for BPD and November 2015 for BCD, but that the regimes had been compliant since those respective dates.[126]

The case was 'an iterative exercise, involving substantial consideration of new facts and issues:'[127] The Tribunal made the following comments on its elucidatory role:

---

[123] *Privacy and Security: A modern and transparent legal framework* (2015) Intelligence and Security Committee HC 1075.

[124] *Privacy International v Secretary of State for Foreign and Commonwealth Affairs* [2017] 3 All E.R. 647, [2016] HRLR 21, at [5]-[8]. This was the first of four legal judgements in the case.

[125] ibid, at [14].

[126] ibid, at [101].

[127] n 122 above, at [6].

> '[…] It is not irrelevant that this Tribunal is called the Investigatory Powers Tribunal, because, in addition to reaching a number of judicial conclusions, it has been constantly necessary, in this case in particular, for the Tribunal… to probe and to consider fresh problems and lacunae.
>
> Both for those reasons and because the Tribunal itself is anxious to assist in achieving improvements in the ways in which the Agencies carry out their responsibilities, there has been a constant increase in the amount of information made available to the public, always subject to the need to balance such openness against the needs of national security. As we have said before, it is important not to identify as the discovery of a failing what is, in fact, the identification of a welcome improvement.'[128]

An important semantic shift had occurred. Before, the name 'Investigatory Powers Tribunal' signified a Tribunal created to settle disputes about investigatory powers; now it signifies a Tribunal that actively investigates.

The publicity function of law

There is no obvious parallel or precedent for the IPT's elucidatory function. It resulted from an evolutionary process of adaptations by judicial bodies under pressure to publicly decide the law in cases where information is subject to legal limitations and where there is pressure from government not to compromise national security by declaring their actions unlawful. In *Malone's case*, when there was no interception legislation in place, legal judgment served to both suspend the trial of the facts, protecting the secrecy of the interception warrant, and to authorise interception operations provisionally until such time as a legislative framework could be constructed. It found a place in the law for a problem that had not previously been asked of a court and secured political time during which legislation could be prepared while interception practices could continue. In retrospect, dealing with the case as a preliminary matter of law served

[128] ibid.

the purpose of avoiding opening the warrant under subpoena. The facts of the situation remained hidden within the envelope of secrecy.

The ICT was a closed system that allowed the government to claim to meet the minimum requirements of the Convention while maintaining control over the secrecy over interception powers. It channelled complaints into a perfectly sealed system, while IOCA's limited scope of review resulted in all complaints being dismissed.

The IPT was supposed to reproduce the form and function of the ICT, but in its 2003 Ruling on preliminary matters of law it opened the way to public arguments about law, insofar as that could be safely abstracted from facts. The ruling was not a binding precedent upon the Tribunal or any other court but there are no reported instances where the IPT declined to hold a hearing when called on to do so.

Snowden's revelations suggested that the powers of the intelligence and security agencies to interfere with privacy had expanded far beyond the opaque descriptions of the RIPA framework. They demonstrated a gap between surveillance powers in practice and what the law described. The Snowden cases before the IPT, with their improvised procedural innovations and self-referential findings, rhyme with *Malone v Metropolitan Police Commissioner* insofar as they served to find a place in the law for inaccessible powers while securing political time to produce updated legislation. No material fault was found to have occurred as result of the law of legal authority, no damages were awarded, and in each case the Tribunal's conclusions ensured that the powers in question could continue operating.

From the perspective of the traditional separation of powers, this appears to blur elements of the judicial, executive, and legislative functions in a troubling manner. The Tribunal's adjudicative role

should, in theory, involve analysing the legal framework and deciding if it is compliant with the Convention or not (the legal/illegal binary). The elucidatory function goes further, with the Tribunal actively shifting the designation. At the second-order level, by deeming the IPT an effective remedy, the ECtHR has also switched assignations: the difference between the Tribunal in *Kennedy* and the Tribunal in *Big Brother Watch* is precisely this evolution from passively reviewing the law to actively intervening in it.

At no point did the Court or Tribunal consider that the government's ability and willingness to withhold information from the public is precisely why there was something there to elucidate in the first place. A cynic could therefore argue that the elucidatory function simply serves to allow governments to ignore their obligations to make accessible and foreseeable rules regarding their use of surveillance powers, improvising to invent rules should they be held to account. In other words, if governments truly respected the Convention's requirements of accessibility and foreseeability then there should be no need for elucidation, a remedy that presupposes governments will exercise powers that are not legally accessible or foreseeable in their effects in defiance of their Convention duties. The Tribunal would then be engaged in a new form of old-fashioned judicial deference to the executive.

That conclusion would be going too far and missing too much. Submissions to the Tribunal show that there was within government a secret framework of rules and procedures around intelligence sharing and a coherent legal argument as to why this was theoretically in accordance with the law. The problem arose from the government's overriding concern for secrecy. In respect of Prism this had a diplomatic dimension, as it concerned the secrecy of an American surveillance system.[129]

[129] This invokes the spectre of the 'control principle'; as defined by the Court of Appeal, it is: "integral to intelligence sharing arrangements that intelligence material provided by one country to another remains confidential

This contextualises the government's argument in *Belhaj* that its findings of illegality should not be publicised. Law is not feared because it places limits on activities that would otherwise be used freely. Indeed, as commentators have argued,[130] the Convention has been interpreted to allow a generous degree of freedom for governments to carry out surveillance. The problem is the publicity that law brings and the risk that, if a finding of illegality was made, it would be followed by complaints from individuals seeking to discover if they had been under unlawful surveillance. That in turn could undermine the purpose of NCND and potentially impact the effectiveness of past or ongoing security and intelligence operations.[131] In short, the rationing of information by the security and intelligence agencies is based on risk, and law is always risky because it decides matters legally, not by reference to dangers that might actualise in the future.

Therefore, once it became clear that the IPT would find the intelligence sharing regime did not comply with the Convention, it became imperative for government to seek to resolve the situation before final judgment was issued. This helps explain why, despite the complainants' objections, the initial finding of illegality in November 2015 was followed by further hearings, Disclosures were drafted and expanded upon in closed sessions, and the updated draft IC Code was laid before Parliament all before the 'open' portion of the case was formally concluded. The Tribunal did not defer to the executive on the law but improvised and collaborated to limit the political risks of its findings.

. . . and that it will never be disclosed . . . without the permission of the provider of the information." *R v. Secretary of State for Foreign & Commonwealth Affairs* [2010] EWCA (Civ) 65, [2010] 3 W.L.R. 554 at [44].

[130] See Hughes, n 1 above; Murphy, n 9 above; and Watt, n 2 above.

[131] This argument was explicitly advanced before the Tribunal in the subsequent case of *Human Rights Watch Inc v Secretary of State for the Foreign and Commonwealth Office* [2016] 5 WLUK 352, [32]-[33].

On the other side, publicity was also in play. The majority of major IPT cases were brought by NGOs, which operate at the interface between law, policy, and media to campaign in the 'public interest'. They require expertise in law, policy, and public relations beyond the capacity of any individual member of 'the public' alone. Following the ruling in the *Liberty v GCHQ* case, Privacy International instigated a web campaign, 'Did GCHQ illegally spy on you?', inviting internet users around the world to complete an online form that would automatically populate and send a complaint form to the IPT on their behalf. If individuals complained of unlawful surveillance under Prism, the Tribunal would be bound to investigate their case. Any interference with privacy caused by GCHQ's use of Prism would have been not in accordance with the law, and the Tribunal would have to uphold their complaints on that basis. This provocative publicity campaign explicitly sought to use the Tribunal to further raise international awareness of surveillance powers. For both sides, for better or worse, the Tribunal served as a strategic publicity device.

In the event, the impact of the campaign was blunted by the ECtHR's findings on admissibility in *Roman Zakharov v Russia*.[132] It held that where there is no domestic effective remedy, then the suspicion that one may be under unlawful surveillance is justified and the Court will admit a complaint without further evidence. Where there are sufficient remedies available domestically, a complaint of surveillance is unlikely to be admitted. The Tribunal thus found that individual complainants now needed to show specific reasons as to why they believe themselves to be victims of unlawful surveillance.[133] This narrows the approach to admissibility laid down in *Klass v Germany*.

---

[132] n 39 above.

[133] n 131 above. In an open judgment on how to deal with the complaints, of which there were in total six hundred and sixty-three, the Tribunal found that only six had provided details as to why they might have been targeted, in addition to the boiler-plate complaints as generated by the Privacy International website. Those six showed personal reasons why they would be at risk of surveillance and an investigation was directed to discover whether they had

In this respect it is perhaps a precursor to the Court's approval of the elucidatory function, which further narrows the scope of admissibility and, by extension, future controversy.[134]

From now on, all complaints from the UK must go via the IPT. If the IPT finds that the general legal framework is not compliant with the accessibility and foreseeability requirements, it can instantly remedy the problem by elucidation. In *Liberty v United Kingdom,*[135] the problem with the IPT was that its public decisions were held not to have binding effect on the UK government. In *Big Brother Watch*, the IPT becomes a one-stop shop: a judicial body that investigates individual complaints, judicially reviews the law, and publishes secret rules and regulations on behalf of the government where required.

Law as a reflexive medium

The elucidatory function is an expression of law's ability to communicate new information about itself in situations where existing provisions are deemed inadequately accessible and foreseeable in their effects. In systems theoretical terms, the norms of 'accessibility' and 'foreseeability' are a product of modern law's reflexivity. Law observes itself as a system that communicates with its environment. Included in its environment is a 'public' that is supposed to access the law and thus

---

been victims of unlawful surveillance. The other applications were dismissed as frivolous under s67(4) RIPA. No further public decisions followed, so it seems reasonable to assume the complaints in respect of the six were 'not upheld'.

[134] *Klass v Germany* [1978] ECHR 4, at [34]: "… an individual may, under certain conditions, claim to be the victim of a violation occasioned by the mere existence of secret measures or of legislation permitting secret measures, without having to allege that such measures were in fact applied to him. The relevant conditions are to be determined in each case according to the Convention right or rights alleged to have been infringed, the secret character of the measures objected to, and the connection between the applicant and those measures."

[135] n 63 above.

foresee the likely use of covert powers that it cannot otherwise know. Who that public is, how it is supposed to know what it should know, and whether any given individual accurately understands and foresees the future correctly are irrelevant matters. Normative questions are defined and answered by the legal system itself. In elucidating previously inaccessible rules, law acts as a medium twice over: it decides what legal information must be communicated to the public, and it publicly communicates its decisions as to why that is so.

In other words, elucidation involves selecting and adding information to the legal system. With systems theory, this can be framed through the concepts of variety and redundancy. Information is 'any difference which makes a difference' to an observing system – it changes the system's state.[136] Once processed, information produces redundancy. Redundancy enables the system to be indifferent to its environment by excluding information, while processing new information with greater complexity and specificity.[137] Increasing thus alters the variety of a system:

> 'redundancy involves the information that is available for the processing of information, and variety is the information that is as yet missing. The greater the variety of a system, the more difficult it becomes to use one operation about which there is little information to draw conclusions about other operations [...] and the more surprises there are to be generated and processed...'[138]

Viewed this way, Snowden's revelations were highly informative and, therefore, surprising. Prior to Snowden, the legal system had little redundancy in respect of the opaque powers he revealed. Variety – the missing information – is why the revelations generated so much legal argument. The

---

[136] G Bateson, *Steps to an Ecology of Mind* (Northvale: Jason Arsonson Inc., 1987) 386; N Luhmann, *Social Systems* n 11 above, 40.

[137] The common law doctrine of precedent serves as an example of the legal system gaining redundancy and thus complexity through its own operations.

[138] n 12 above, 320. Note that Luhmann cautions against understanding redundancy and variety as binary opposites.

informational content of the law was shown to be deficient. Elucidation, as the production of more information, is the production of redundancy.

Conclusion: no alarm, no surprises

As shown by the timing of events in the hacking and bulk dataset cases, the IPT's ruling in February 2015 inaugurated a change in government policy. Initially the government responded to the Snowden revelations with NCND and argued that everything it did was in accordance with the law. The shift to elucidation ultimately resulted in the Investigatory Powers Act 2016. The Act means it is improbable that the elucidatory function will be required again soon in relation to communication surveillance powers in the UK.

Procedurally, the creation of a right to appeal against decisions of the IPT to the Court of Appeal lowers the pressure on the Tribunal to fully resolve complex questions of law through procedural improvisation. But in terms of accessibility and foreseeability, the IPA is like an open book of surveillance powers compared to its predecessors.[139] While IOCA, the Security Service Act 1989, and the Intelligence Services Act 1994 brought covert national security powers onto a legal footing during the 1980s and 1990s,[140] the statutes were deliberately opaque as to the powers that they authorised.[141] By contrast, each of the controversial surveillance techniques revealed by Snowden is now clearly described, with a list of specific safeguards, in its own chapter of the IPA.

---

[139] For a list of judicial dicta describing the difficulty of understanding the 'labyrinthine' RIPA, Graham Smith, 'Future-Proofing the Investigatory Powers Bill', (15th April 2016, *Cyberleagle* blog) at http://www.cyberleagle.com/2016/04/future-proofing-investigatory-powers.html .

[140] L Lustgarten and I Leigh, *In from the Cold: National Security and Parliamentary Democracy* (Oxford: Oxford University Press, 1994) is the classic account, see also C Moran, *Classified: Secrecy and the State in Modern Britain* (Cambridge: Cambridge University Press, 2012), 25.

[141] See Glover, n 33 above, 11-12.

With the IPA, the law has greatly increased in redundancy. As such, it reduces the risk of the system being surprised by unexpected information in the future. The elucidatory function will not be required, but it remains as an approved legal procedure, an insurance mechanism for absorbing surprises, insulating the political system from legal scandal. In effect, it means it is no longer possible for a legal regime governing secret powers to be 'not in accordance with the law'. Any challenge to that effect will inevitably begin a process of communicating more information from 'below the waterline', adding redundancy to the system, neutralising the problem. Should the government ever again be surprised by unexpected disclosures like Snowden's, the Tribunal will simply elucidate the position.