Transparency and surveillance: assessing the approach of the Investigatory Powers Tribunal in Liberty & Others

Article *in* Public law · January 2016

CITATIONS
0

READS
256

1 author:

Maria Helen Murphy
National University of Ireland, Maynooth
18 PUBLICATIONS **35** CITATIONS

SEE PROFILE

Transparency and surveillance: assessing the approach of the Investigatory Powers Tribunal in *Liberty & Others*

Maria Helen Murphy

Introduction

A recent pair of Investigatory Powers Tribunal (IPT) rulings—involving privacy advocates, the Intelligence Service (MI5), the Secret Intelligence Service (MI6), and the Government Communications Headquarters (GCHQ)— raises pressing questions about the importance of transparency in the surveillance context.[1] Through Edward Snowden's exposure of the covert activities of intelligence agencies, unwanted transparency was imposed on many of the world's most powerful governments. In fact, the original basis for the complaints ruled on by the IPT arose from documents made public as a direct result of the Snowden revelations. A tension exists between the reality that full transparency of intelligence activities could hinder the effectiveness of such operations and the principle that transparency is essential if citizens are to hold their government to account accurately.[2] This article examines the struggle between these competing ideas and considers how the IPT resolved the tension. In conclusion, this article speculates on how the European Court of Human Rights (ECtHR) might resolve the conflict differently and suggests the adoption of an evolved approach that values transparency but does not rely on it as a panacea.

From the decision not to admit the existence of MI6 until 1994,[3] to the governance of the intelligence services through informal non-statutory mechanisms for many years,[4] the United Kingdom intelligence services have historically fostered a strong culture of secrecy. This legacy of opacity has significantly lessened in recent decades as British society has witnessed the gradual opening up of covert intelligence activities to public scrutiny.[5] The key incentive for such reform, however, has not been recognition of the benefits of transparency in a democratic society, but a desire to avoid legal challenge.[6] The threat of legal challenge arose primarily from obligations under the European Convention on Human Rights (ECHR).[7]

Of course, the UK intelligence agencies are not alone in seeking to shield their activities from scrutiny and this can be defended in certain circumstances. There is clearly a legitimate interest in protecting the operational methods of intelligence agencies from complete transparency. An obvious case for reduced transparency occurs in the surveillance context, where the effectiveness of investigations would be reduced if targets had enough information to consistently evade surveillance. In the seminal case of *Malone*, the ECtHR displayed an appreciation of the importance of secrecy in the context of surveillance activities by stating

---

[1] *Liberty, Privacy International, American Civil Liberties Union, Amnesty International, and Bytes For All v The Government Communications Headquarters, the Secretary of State for the Foreign and Commonwealth Office, and the Security Service* [2014] UKIPTrib 13_77-H; *Liberty & Others v The Secretary of State for Foreign and Commonwealth Affairs & Others* [2015] UKIPTrib 13_77-H.

[2] Albert Meijer, "Understanding modern transparency" (2009) 75(2) Int'l Rev.Admin.Sci. 255.

[3] Helen Fenwick, *Civil Liberties and Human Rights* (London: Cavendish, 2002), p.649.

[4] See fn.3, p.649. In 1987, Anthony Duff persuaded the Home Secretary at the time, Douglas Hurd, that "the time had passed when the Security Service could successfully operate on the basis that it did not exist" as the pretence had worn "threadbare". Christopher Andrew, *The Defence of the Realm: The Authorized History of* MI5 (London: Penguin, 2010), p.766.

[5] Benjamin Goold, "Liberty and others v The United Kingdom: a new chance for another missed opportunity" [2009] P.L. 5, 5.

[6] See fn.5 and fn.3, p.650.

[7] Mike Maguire, Timothy John, "Covert and deceptive policing in England and Wales: Issues in regulation and practice" (1996) 4 Eur. J. Crime Cr. L. Cr. J. 316, 317.

> "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".[8]

Crucially, however, the ECtHR went on to state that the law governing surveillance activities must indicate the scope of the discretion allowed to the authorities and the manner of its exercise with "sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference".[9] The ECtHR concluded that the UK law governing interception did not meet this standard.[10] The decision in *Malone* was a key catalyst for increased transparency of UK surveillance procedures and was a direct influence on the development of the Interception of Communications Act 1985.[11] While the Interception of Communications Act 1985 has been criticised for constituting an unsatisfactory approach to compliance in response to the judgment in *Malone*,[12] it was significant as the first attempt to provide a statutory framework for the interception of communications.[13] Similarly, it has been argued that the provision of a legal basis for the use of surveillance devices by police in Part III of the Police Act 1997 was only introduced when it was clear that the UK would lose a ECtHR case challenging the use of such devices.[14] The introduction of comprehensive surveillance legislation, in the form of the Regulation of Investigatory Powers Act 2000 (RIPA), has been represented as another example of the UK government increasing the transparency of its surveillance operations in response to the demands of Convention compliance.[15]

Another relevant reform to the activities of intelligence agencies was the creation of the IPT, which was established by s. 65 of RIPA. The IPT is "the only appropriate tribunal" for the purposes of s. 7 of the Human Rights Act 1998 in relation to any proceedings against the intelligence services relating to actions incompatible with the ECHR.[16] Accordingly, the IPT is the only tribunal where the surveillance activities of the intelligence agencies can be challenged on ECHR grounds. Unsurprisingly, the IPT was not established to open the activities of the intelligence agencies to full scrutiny, the imperative of secrecy was deemed too great. While the provision of a tribunal providing some accountability and access to remedies for surveillance targets is a positive feature of the UK system, an inherent flaw in its effectiveness has been the fact that investigative authorities have no obligation to notify individuals who have been subjected to surveillance.

The two recent rulings of the IPT

The background to these rulings is now well-known. While former intelligence insiders had made similar claims before the Snowden leaks, the publication of official documents provided an inescapable tangibility that captured the public imagination, removed the option of plausible deniability from the surveillance agencies, and put the issue of privacy firmly back on the

[8] *Malone v UK* [1984] E.C.H.R. 10 at 67.
[9] See fn.8 at 68.
[10] See fn.8 at 79.
[11] See fn.13 below, 69; see fn.46 below, Ch.3.
[12] See fn.7, 321; Bethan Loftus, Benjamin Goold and Shane Macgiollabhui, "Covert policing and the Regulation of Investigatory Powers Act 2000" (2010) 8 Arch. Rev. 5.
[13] Nick Taylor, "State surveillance and the right to privacy" (2002) 1(1) Surveill. Soc. 66, 69.
[14] *Khan v UK* (2001) 31 E.H.R.R. 1016. Legislation regulated telephone tapping following *Malone*, but bugging remained regulated by Home Office Guidelines. See fn.13, 70; Keir Starmer, Michelle Strange and Quincy Whitaker, *Criminal Justice, Police Powers and Human Rights* (London: Blackstone, 2001), p.36.
[15] Jack Straw claimed that RIPA was "a significant step forward for the protection of human rights in this country" Hansard, HC vol.345, col.767) (March 6, 2000). See fn.13, 72.
[16] Regulation of Investigatory Powers Act 2000 s.65.

global agenda. The UK and its intelligence agencies were the subject of a significant number of documents disclosed in the Snowden leaks. In fact, Snowden himself has commented that mass surveillance is "not just a US problem ... the UK has a huge dog in this fight".[17] Snowden has gone so far as to claim that GCHQ "are worse than the US".[18] Human Rights groups—including Liberty and Privacy International—seized the opportunity provided by the Snowden leaks in order to challenge the activities of the UK intelligence agencies. The specific activities challenged in the two recent IPT rulings concern the arrangement that provided for UK intelligence agency access to US surveillance materials gathered through the operation of the controversial "PRISM" and "Upstream" surveillance programmes. While some aspects of the initial media reports concerning these programmes have been criticised,[19] a report by the Privacy and Civil Liberties Oversight Board (PCLOB) provides a credible insight into what these systems entailed.[20] According to the PCLOB, US intelligence agencies sent written directives to electronic communication service providers that had been served with s. 702[21] directives requiring their assistance.[22]

The PRISM system involves the government sending selectors (such as email addresses) to electronic communication service providers based in the US (including Facebook and Microsoft) and compelling the service provider to supply the government with all communications sent to or from that selector.[23] Upstream collection occurs by compelling those who control major communications cables and switches to share communications which are deemed likely to contain foreign communications. This led to the acquisition of millions of communications, including emails and social media posts, which were then filtered through the use of selectors. While both PRISM and upstream collection have been criticised in the US, for the purposes of this article, the arrangement permitting UK access to these communications is the most pertinent issue.

The arrangement that governed this information sharing between US and UK intelligence agencies was secret prior to the Snowden revelations. Further details of the arrangement were revealed in the course of the IPT proceedings. According to disclosures made by the respondents on foot of the complaint, UK intelligence agencies may request access to communications intercepted by foreign allies without the use of any international mutual legal assistance agreement in two circumstances.[24] It was disclosed that they may obtain the communications if an interception warrant has been issued under the RIPA, the assistance of the foreign government is necessary to obtain the communications, and it is necessary and proportionate to do so.[25] The IPT proceedings also revealed that the intelligence services may obtain the communications without a RIPA interception warrant if the obtaining would not

[17] Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies and James Ball, "GCHQ taps fibre-optic cables for secret access to world's communications" (June 21, 2013) *The Guardian*, *http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa*.
[18] See fn.17.
[19] Joe Svetlik, "Doubts cast on US govt Prism snooping program" (June 8, 2013) *CNET*, *http://www.cnet.com/uk/news/doubts-cast-on-us-govt-prism-snooping-program/*.
[20] See fn.22 below. While factually authoritative, its analysis has been challenged. Mike Masnick, "Privacy And Civil Liberties Board mostly unconcerned about PRISM or backbone tapping by NSA" (July 2, 2014) *Tech Dirt*, *https://www.techdirt.com/articles/20140702/06315727755/privacy-civil-liberties-board-mostly-unconcerned-about-prism-backbone-tapping-nsa.shtml* .
[21] Foreign Intelligence Surveillance Act (1978) as amended s.702.
[22] Privacy and Civil Liberties Oversight Board (PCLOB), *Report on the surveillance program operated pursuant to section 702 of the Foreign Intelligence Surveillance Act* (2014), p.7.
[23] See fn.22.
[24] *Liberty & Others* [2014] UKIPTrib 13_77-H at 47.
[25] See fn.24.

amount to a "deliberate circumvention of RIPA"[26] and the obtaining was necessary and proportionate.[27]

Due to the secret nature of both the information sharing arrangement and the PRISM and Upstream programmes, it is unsurprising that UK human rights groups launched a legal challenge following the Snowden revelations. The basic complaint made to the IPT was that the secret arrangement between GCHQ and the National Security Agency violated Articles 8 and 10 ECHR. While freedom of expression has clear ancillary relevance to the claim, the focus of both rulings was on whether Article 8 had been violated. While Article 8 guarantees a right to respect for private life, that right is limited in circumstances where the limitation is "in accordance with the law", "for a legitimate aim", and "necessary in a democratic society". The focal point of both the December 2014 and February 2015 rulings was whether the information sharing arrangement between the US and UK intelligence agencies was "in accordance with the law". The focus on the "in accordance with the law" aspect of the inquiry, at the expense of the "necessary in a democratic society" question, is unsurprising in light of the tendency of the ECtHR to adopt a similar approach when dealing with surveillance cases.[28]

When determining whether an interference with Article 8 was "in accordance with the law", the ECtHR examines whether the intrusive measures have a basis in domestic law[29] and whether the law was adequately accessible and foreseeable.[30] These requirements are logical protections as when actions are obscured from public scrutiny, there is an increased risk of arbitrariness.[31] In the December 2014 and February 2015 rulings, the IPT reflected this approach, and stated that in order for an interference with Article 8 to be deemed "in accordance with the law", the

> "law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference."[32]

The IPT placed significant emphasis on the importance of foreseeability of surveillance measures and stated that "sufficient signposting of the rules or arrangements" is required. The key finding of the December ruling was that the arrangement that allowed UK intelligence agencies access to surveillance information garnered from the US PRISM and Upstream programmes was compliant with the ECHR. The IPT acknowledged, however, that where such arrangements are secret, they will not be sufficiently accessible to the public. As accessibility and foreseeability are both key requirements of the ECHR, the formerly secret nature of the US–UK arrangement was inherently problematic. An interesting aspect of the ruling was the finding by the IPT that an adequate indication of the arrangement had been provided by virtue of information released following the commencement of the legal action. This "signposting" was primarily comprised of a summary of the sharing arrangement as reported in the public rulings of the IPT. The inference of this finding is that the "in accordance with the law" deficiencies of the surveillance arrangement were remedied by the transparency effectively imposed on the agencies through the pursuit of legal redress.

---

[26] Or otherwise contravene the Padfield principle, e.g. where obtaining the communications under RIPA would not be technically feasible.
[27] See fn.24. According to the respondents, in the second circumstance, the Secretary of State would have to approve the request personally.
[28] See fnn.47-48 below.
[29] See fn.8 at 79; *Khan v The United Kingdom* (2001) 31 E.H.R.R. 1016 at 27-28.
[30] See fn.8 at 67; *Valenzuela Contreras v Spain* (1999) 28 E.H.R.R. 483 at 46; *Ekimdzhiev v Bulgaria* [2007] E.C.H.R. 533 at 71.
[31] See fn.8 at 67; *Klass* (1979-80) 2 E.H.R.R. 214 at 42-49; *Ekimdzhiev* [2007] E.C.H.R. 533 at 71.
[32] See fn.24 at 37; See fn.34 below at 15. Both rulings citing *Bykov v Russia* [2009] E.C.H.R. 441 at 76-78.

This would appear to be a cruel twist of fate for the privacy advocates and non-governmental organisations who had made the complaint to the IPT, on foot of the Snowden revelations, and had resultantly forced the intelligence agencies to reveal the arrangement to the IPT. It would certainly seem to be unsatisfying for this forced disclosure to now enable the intelligence agencies to assert the human rights compliance of their surveillance activities. The incongruity of this finding was mitigated somewhat by a nuance in the December ruling which saw the IPT question whether a finding of compliance would have been possible without the benefit of disclosures unwillingly made by the intelligence agencies.[33] In line with this, the Order to the December judgment directed the parties to serve written submissions with a view to resolving

> "[w]hether by virtue of the fact that any of the matters now disclosed in the judgment of 5 December 2014 were not previously disclosed, there had prior thereto been a contravention of Articles 8 or 10 ECHR."[34]

Put simply, the IPT wished to address whether the surveillance arrangement had been in violation of the ECHR prior to the December ruling.

Following due consideration of the submissions, the IPT ruled in February that prior to the disclosures made and referred to in the IPT's December 2014 and February 2015 rulings, "Prism and/or Upstream arrangements contravened Articles 8 or 10 ECHR, but now comply".[35] While this holding was a valuable concession to the complainants' case, it was couched in a general finding of legality. The mixed nature of the ruling has been appropriately reflected in the public statements of the parties made in response. A GCHQ spokesperson played down the significance of the ruling and focused on the finding of legality:

> "We are pleased that the court has once again ruled that the UK's bulk interception regime is fully lawful. It follows the court's clear rejection of accusations of 'mass surveillance' in their December judgment."[36]

In a stance of defiance, the spokesperson asserted that the ruling would "not require GCHQ to change in any way what it does".[37] On the other hand, the February ruling was the first example of the IPT finding against the intelligence services in the Tribunal's 15-year history. Clearly, this alone constituted a significant victory for transparency and the protection of privacy. Eric King, of Privacy International, expressed thanks to Edward Snowden for exposing the secret surveillance activities and described the decision of the IPT as a "vindication of his actions".[38] The ruling has also been described as "a validation—if such still were needed—of the importance of the document releases from Snowden".[39] In spite of such endorsements, it is clear to all that the victory for privacy in these rulings is, at best, a partial one. The finding that the subsequent—non-voluntary—disclosures are deemed sufficient to bring the system into compliance clearly tempers the value of the result from a privacy perspective. A further effect of the ruling, however, is to add purpose to the pursuit of the UK intelligence agencies at the ECtHR. In response to the ruling, James Welch, Legal Director for Liberty, expressed

---

[33] See fn.24 at 153-154; See fn.34 below.
[34] *Liberty & Others* [2015] UKIPTrib 13_77-H at 11.
[35] See fn.34 at 32.
[36] Owen Bowcott, **"**UK-US surveillance regime was unlawful 'for seven years'" (February 6, 2015) *The Guardian*, *http://www.theguardian.com/uk-news/2015/feb/06/gchq-mass-internet-surveillance-unlawful-court-nsa*.
[37] See fn.36.
[38] Privacy International, "GCHQ-NSA intelligence sharing unlawful, says UK surveillance tribunal" (February 6, 2015) *privacyinternational.*org, *https://www.privacyinternational.org/?q=node/482*.
[39] Karlin Lillington, "Ruling on data spying validates Snowden's actions" (February 27, 2015) *The Irish Times*, *http://www.irishtimes.com/business/technology/ruling-on-data-spying-validates-snowden-s-actions-1.2100158*.

satisfaction with the finding of a violation but stated that Liberty disagrees with the holding that the safeguards revealed during IPT proceedings are adequate for the protection of privacy and expressed resolve to pursue the issue to Strasbourg.

Likelihood of success at the ECtHR

It is submitted that the contention of the complainants that the "forced disclosure of a limited subset of rules" governing mass surveillance is insufficient to render the activities lawful has merit. As the ECtHR has consistently stated, in order for intrusive surveillance measures to be found compatible with Article 8, the legal basis for the intrusive measures must be adequately accessible and foreseeable.[40] The conclusion reached by the IPT that the recently publicised summary of the internal policies—as contained in a 77-page decision of the IPT and not enshrined in statute[41]—constituted a sufficiently detailed and public legal framework is ripe for challenge.

While the ECtHR has previously held that not all government endorsed privacy intrusions require publication in statute,[42] such publication would clearly be desirable from the perspective of accessibility and foreseeability. Even assuming the ECtHR does not find statutory enshrinement to be necessary, there is a strong argument that the limited description of the arrangement, and its basis in a complex collection of various legal grounds and interpretations, fails to provide 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".[43]

Supporters of the legal action have a long line of decisions from the ECtHR jurisprudence that support their focus on the "in accordance with the law" standard. Notably, the ECtHR has censured the UK government numerous times for failing to provide adequate accessibility and foreseeability of the laws governing its surveillance procedures. In the case of *Liberty*, the ECtHR ruled that in spite of the existence of "internal regulations, manuals and instructions to provide for procedures to protect against abuse of power" the law had not 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".[44]

Due to the prominent role that the "in accordance with the law" standard has played in the surveillance jurisprudence, it seems likely that the ECtHR may find against the UK on similar grounds yet again. If the ECtHR finds against the UK, the Court may choose to delineate the requirements of a surveillance sharing regime that would meet the appropriate standard of accessibility and foreseeability. In the past, the ECtHR has not hesitated to be prescriptive in this regard.[45]

There are clear benefits to focusing on the "in accordance with the law" question in the surveillance context. Lustgarten and Leigh point out that framing laws with precision announces not only to the relevant authorities, "what practices are authorized, for what

[40] See fn.30.
[41] Eric King, Carly Nyst and Caroline Wilson Palow, "The snoopers' loophole: why winning against GCHQ is bittersweet" (February 10, 2015) *privacyinternational.org*, *https://www.privacyinternational.org/?q=node/494*.
[42] *Kruslin v France* (1990) 12 E.H.R.R. 547 at 29.
[43] See fn.8.
[44] *Liberty v UK* [2008] E.C.H.R. 568 at 66-69
[45] *Huvig v France* (1990) 12 E.H.R.R. 528 at 34; see fn.43 at 35; *Valenzuela Contreras* (1999) 28 E.H.R.R. 483 at 46; *Weber and Saravia v Germany* [2006] E.C.H.R. 1173 at 95.

purposes, and within what limits" but also communicates this clearly to the public.[46] Evidence for ECtHR support of this view is found in the surveillance context, where the ECtHR has often found a violation under the legality test and then chosen not to consider the question of necessity.[47] This focus contrasts with the approach of the ECtHR in other contexts, where the ECtHR has often focused its scrutiny on the "necessary in a democratic society" question.[48]An advantage of assessing the surveillance regime under the "in accordance with the law" test is that the ECtHR can avoid thorny questions of national interest and the margin of appreciation. This has clear appeal in an area of such acutely sensitive national interest as focusing on requirements of accessibility and foreseeability inures the ECtHR from being criticised for making "arbitrary value judgments".[49]

It is worth reflecting on the fact, however, that while the jurisprudence of the ECtHR in surveillance cases has been "traditionally hailed as a powerful demonstration of the strength of the Convention",[50] the responses to these rulings have been criticised as minimalist.[51] While the UK has frequently responded to European developments in privacy law with reform measures, Goold points out that the amendments have tended to be "uniformly backward-looking and begrudging" with the focus on protecting surveillance powers while affecting the role of compliant state.[52] Accordingly, while it seems likely that the civil liberties groups will have success in Strasbourg, there is a risk that it will be on similarly—if not quite so—narrow grounds as the February ruling of the IPT. The historical response of the UK to such findings in similar circumstances inspires scepticism regarding the privacy enhancing benefits of such a decision.

Conclusion

The civil liberties campaigners involved in the action against the UK intelligence agencies extol the virtues of transparency. The ECtHR approach to accessibility and foreseeability attempts to draw the appropriate balance between the importance of secrecy in covert investigations and the democratic imperative for transparency of government actions and powers. A clear point of contention regarding the recent rulings of the IPT was the finding that surveillance conducted after January 2015 was acceptable as the formerly secret rules have been made public through the legal proceedings. The irony of the new-found transparency being largely attributable to the Snowden revelations is evident. The interception sharing arrangement was in violation of the Convention when it was conducted in secret, but the exposure of the programme—and consequent summary explanation of the arrangement—remedied the illegality and rendered the arrangement compliant. Such a finding undermines the

[46] Laurence Lustgarten and Ian Leigh, *In from the cold: National security and parliamentary democracy* (Oxford: Clarendon Press, 1994), p.46.
[47] Nicole Moreham, "The right to respect for private life in the European Convention on Human Rights: a re-examination" [2008] E.H.R.L.R. 44, 55-56; Iain Cameron, *National security and the European Convention on Human Rights* (The Hague: Kluwer Law International, 2000), p.102; Rita Esen, "Intercepting communications 'in accordance with the law'" [2012] J. Crim. L. at 164.
[48] This is in spite of the fact that finding a breach under the first or second standard of Article 8 will often "obliterate the need for evaluations based on the third standard". Pieter Van Dijk, Fried van Hoof, Arjen van Rijn and Leo Zwaak, *Theory and practice of the European Convention on Human Rights* (Antwerp: Martinus Nijhoff, 2006), p.334-335. Yutaka Arai-Takahashi, *The margin of appreciation doctrine and the principle of proportionality in the jurisprudence of ECHR* (Antwerp: Intersentia, 2002), p.62; Stefan Sottiaux, *Terrorism and the limitation of rights* (Oxford: Hart, 2008), p.276.
[49] Aileen McHarg, "Reconciling human rights and the public interest: conceptual problems and doctrinal uncertainty in the jurisprudence of the European Court of Human Rights" (1999) 62(5) M.L.R. 671 at 671.
[50] Antoine Hol and John Vervaele, *Security and civil liberties: the case of terrorism* (Antwerp: Intersentia, 2005), pp.45-46.
[51] See Fn.5, 5-6.
[52] See Fn.5, 5-6.

promise of transparency as a tool of government control. While transparency is necessary, it is certainly not the solution. Where transparency reveals activities with serious implications for the private life of citizens, it is imperative that the proportionality and reasonableness of such programmes are given full consideration. Without such assessment, a requirement of transparency becomes a minor hurdle for the government to overcome and provides a veneer of legitimacy to what may be excessive and undemocratic programmes.

The case of *Marper* offers an alternative roadmap for the ECtHR to follow when it considers the Convention compliance of the US–UK arrangement. In *Marper*, the ECtHR could have found the DNA Database system to be in breach of the ECHR on legality grounds as "[a]ll the significant detail about operation of the DNA and fingerprint database … was contained in non-statutory internal guidance".[53] Instead, however, the ECtHR chose to focus on questions of reasonableness and concluded that the DNA Database regime constituted "a disproportionate interference with the applicants' right to respect for private life and cannot be regarded as necessary in a democratic society".[54] While the application of the "in accordance with the law" test has clear benefits in such sensitive areas of government policy, its consideration should not be at the expense of the necessity test. Where review is limited to whether an adequate legal basis is provided, the political questions are ignored and the review strays dangerously close to tokenism.[55] After all, the UK government could, yet again, respond to such a finding with a minimalist law and continue or even increase its current activities. In line with this reasoning, the ECtHR should reject the easy option and embrace a full consideration of the proportionality of the information sharing arrangement.

[53] Gordon Nardell, "Levelling up: data privacy and the European Court of Human Rights" in Serge Gutwirth, Yves Poullet and Paul de Hert (eds), *Data Protection in a Profiled World* (Amsterdam: Springer, 2010).
[54] *S and Marper v UK* [2008] E.C.H.R. 1581 at 125.
[55] In spite of this risk, the cases of *Iordachi* and *Ekimdzhiev* provide useful demonstrations of the "in accordance with the law requirement" being applied in a more effective manner. In addition to assessing the sufficiency of the legislative safeguards in place, the ECtHR also evaluated the effectiveness of the regimes in practice by examining the number of warrants issued. According to the ECtHR in *Ekimdzhiev*, the numbers indicated that the system of secret surveillance was "to say the least, overused, which may in part be due to the inadequate safeguards which the law provides". *Ekimdzhiev* [2007] E.C.H.R. 533 at 92 and *Iordachi v Moldova* [2009] E.C.H.R. 256 at 52.