Effective Oversight of Large-Scale Surveillance Activities: A Human Rights Perspective

Daragh Murray*, Pete Fussey**, Lorna McGregor***, &
Maurice Sunkin QC (Hon)****

INTRODUCTION

Today, state surveillance involves the large-scale monitoring, collection, and analysis of digital information. Recent exponential developments in this area have been facilitated by the transition from analogue to digital forms of communication, and technological innovations such as the use of machine learning and artificial intelligence techniques for the ordering, triaging, and analysis of data. This form of surveillance activity makes possible near-population level monitoring and is used, for example, to surface individuals of potential interest to

* Senior Lecturer, University of Essex. Deputy workstream lead, Human Rights, Big Data & Technology Project. The authors' work was supported by the Economic Social and Research Council, grant number ES/M010236/1.

** Professor of Sociology, University of Essex. Research Director, Human Rights, Big Data & Technology Project.

*** Professor of International Human Rights Law, Director Human Rights, Big Data & Technology Project, University of Essex.

**** Professor of Public Law and Socio Legal Studies, University of Essex.

intelligence analysts, to identify and uncover networks, or to create in-depth individual profiles.

To date, commentary on the legality and legitimacy of bulk surveillance regimes has focused on whether the routine surveillance of large numbers of individuals is permissible, in and of itself. However, in several recent cases, the European Court of Human Rights (ECtHR) has held that, in principle and subject to appropriate safeguards, bulk surveillance regimes *may* form a legitimate part of states' response to national security threats.[1] The significance of this is that courts will now have to undertake two tasks. First, to ensure human rights compliance, they must in each case continue to examine whether states' bulk surveillance activity is "in accordance with the law," whether it pursues a legitimate aim, and whether it can be considered necessary, or strictly necessary, in a democratic society.[2] Second, as part of the necessity test, they must now also examine whether an "effective" oversight mechanism has been established,[3] raising key questions as to the nature, composition and practice of such mechanisms. Identifying and understanding the – still developing – human rights law requirements with respect to how large-scale surveillance oversight mechanisms are established, and how they operate in practice, is the focus of this article.

The ECtHR has found that, if large-scale surveillance regimes are to exist, it is essential that "adequate and effective guarantees against abuse"[4] – such as an effective oversight mechanism[5] – are in place to ensure that any interference with human rights is limited to that which is necessary, or strictly necessary, "in a democratic society."[6] As such, ensuring "adequate and effective guarantees against abuse" requires clarity on the formal mandate and composition of an oversight mechanism, as well as an understanding of the measures necessary to deliver this mandate. The difficulty, however, is that the literature and case law provide very little guidance on the nature of oversight bodies in general.[7] In

1. *See*, *e.g.*, Big Brother Watch v. United Kingdom, App. Nos. 58170/13, 62322/14, & 24960/15, ¶ 314 (Sept. 13, 2018), https://perma.cc/VQH5-D2DW; Centrum for Rättvisa v. Sweden, App. No. 35252/08, ¶ 104 (June 19, 2018), https://perma.cc/C3NV-48QM. The case of Big Brother Watch is currently pending before the Grand Chamber of the European Court, and so it is possible that certain conclusions as to the legitimacy of large-scale surveillance regimes, or aspects thereof, may be reconsidered.

2. The precise test is currently unclear. Typically, interferences with rights must be deemed 'necessary' in a democratic society. However, long standing case law indicates that large scale secret surveillance activity must pass a higher threshold of 'strict necessity.' *See, e.g.*, Rotaru v. Romania, 2000-V Eur. Ct. H.R. 109, ¶ 47; Szabó v. Hungary, App. No. 37138/14, ¶ 54 (Jan. 12, 2016), https://perma.cc/UZK6-EAQA; c.f. *Big Brother Watch*, App. Nos. 58170/13, 62322/14, & 24960/15, ¶ 308 (referring only to a 'necessity' test).

3. *See, e.g.*, Zakharov v. Russia, App. No. 47143/06, ¶ 232 (Dec. 4, 2015), https://perma.cc/7MK4-LKXD; *Big Brother Watch*, App. Nos. 58170/13, 62322/14, & 24960/15, ¶ 387.

4. *Rättvisa*, App. No. 35252/08, ¶ 104.

5. *See*, *e.g.*, *Big Brother Watch*, App. Nos. 58170/13, 62322/14, & 24960/15, ¶ 318.

6. *Rättvisa*, App. No. 35252/08, ¶ 104.

7. This article draws heavily on comparative literature and case law relevant to the operation of courts or commissions of inquiry addressing national security issues, such as the Foreign Intelligence Surveillance Act (or FISA) Courts in the United States, immigration tribunals in the United Kingdom, or the Arar commission in Canada. Academic commentary on surveillance oversight has steadily grown in

particular, there has been insufficient analysis of central questions regarding the stages at which oversight takes place (that is, pre, during, or post-operation); how these stages of oversight relate to each other; and what is required to ensure that oversight mechanisms operate effectively and independently in practice. Nor has sufficient attention been given to the form the oversight mechanism should take, for example should it be a court, a judge-led process, or a body such as a parliamentary committee? As such, serious questions arise as to whether, and to what extent, it is possible to establish oversight mechanisms that meet the requirements of international human rights law.

This article seeks to make a key contribution to the literature on oversight generally and bulk surveillance specifically. It suggests elements that an oversight mechanism should incorporate to both ensure its compliance with international human rights law and to facilitate its effective operation in practice. Some of these, such as the need for independence, emerge clearly from the relevant case law. Others, such as the suggestion that judge-led bodies, but not courts, are best placed to conduct oversight, or that points of friction be built into the oversight process, are more contentious. It is these elements, and consideration as to how to ensure that oversight "works" in practice, that represent the added value of this article. The proposals presented here are based on an analysis of existing case law and academic discussion of surveillance oversight. They are also empirically informed by a series of workshops on surveillance oversight, which brought together intelligence oversight bodies, current and former intelligence actors, civil society, academics, and lawyers.[8]

Oversight mechanisms typically engage in activities such as reviewing or approving warrants, examining specific case files (potentially through random sampling), conducting thematic investigations, or monitoring specific surveillance operations. Oversight activity is roughly divided into three inter-dependent, but necessarily distinct, stages: authorization, ongoing supervision of surveillance

---

the wake of Edward Snowden's revelations during June 2013. Variants of this literature have emphasized, among others, the broad drivers of collection of processes grouped together as 'surveillance policy,' *see* Arne Hintz & Lina Dencik, *The Politics of Surveillance Policy: UK Regulatory Dynamics after Snowden*, 5 INTERNET POL'Y REV., Sept. 2016, the legal landscape as it applies to authorising distinct surveillance practices, IAN BROWN, MORTON H. HALPERIN, BEN HAYES, BEN SCOTT & MATHIAS VERMEULEN, TOWARDS MULTILATERAL STANDARDS FOR SURVEILLANCE REFORM, OXFORD INTERNET INST. DISCUSSION PAPER (2015), specific surveillance tools, *see* Daniel Trottier, *Open Source Intelligence, Social Media and Law Enforcement: Visions, Constraints and Critiques*, 18 EUR. J. CULTURAL STUD. 530 (2015), and attention to varied stakeholders in the complex governance structures of surveillance oversight, *see* Hintz & Dencik, *supra* note 7. As the discussion below elaborates, gaps remain in two key areas: attention to post-authorisation practices and more detailed analysis of the delineation of oversight practices into specific tasks and phases.

8. *See* HUM. RIGHTS, BIG DATA & TECH. PROJECT, *Investigating How Intelligence Oversight Techniques are Being Used and Their Utility in Protecting Human Rights* (Mar. 15, 2021), https://perma.cc/2ZHH-5DMA; INVESTIGATORY POWERS COMM'R'S OFF., *IPCO Collaboration with the University of Essex by Legal & Policy Team* (May 30, 2018), https://perma.cc/M4T4-CR35. Some of the authors have also engaged in a separate, closed workshop convened by the Five Eyes Oversight Mechanisms.

activities, and ex post facto review.[9] This article addresses the first two elements of this process as they raise a number of novel and practice-oriented issues in a bulk surveillance context. Ex post facto review – and in particular the provision of an effective remedy – is necessarily an essential component of any oversight regime,[10] but raises distinct issues beyond the scope of this paper, and is therefore only discussed in terms of its relationship to the ongoing supervision stage.

A number of different types of oversight mechanisms exist.[11] This article focuses on judge-led mechanisms with the authority to issue binding decisions. This focus is based on consistent ECtHR case law stating that "it is in principle desirable to entrust supervisory control to a judge, judicial control offering the best guarantee of independent, impartiality, and a proper procedure."[12] However, as discussed in Section I(A) below, the focus is not exclusively on judicial bodies (or courts) in the traditional sense, in recognition of the fact that judicial control is not necessarily sufficient of itself, and that "regard must be had to the actual operation of the system of interception, including the checks and balances on the exercise of power, and the existence or absence of any evidence of actual abuse."[13] The analysis draws from recent innovations in the U.K. regulatory landscape, most notably the establishment of the Investigatory Powers Commissioner's Office (IPCO), the U.K. body established to oversee large-scale covert surveillance activity by the Investigatory Powers Act 2016.[14] This is not to suggest that IPCO represents an "ideal" oversight body; a number of shortcomings are discussed below. Rather, this is a newly established oversight body which provides an appropriate reference point against which to test the human rights law requirements elaborated over the course of this article. Other non-judicial mechanisms, including parliamentary oversight committees, can play an important role, particularly in relation to public scrutiny and political supervision. However, these mechanisms are arguably most effective when established to

9. *See, e.g.*, Zakharov v. Russia, App. No. 47143/06, ¶ 233 (Dec. 4, 2015), https://perma.cc/7MK4-LKXD. Ex post facto review is the review conducted after the surveillance operation has terminated and may.

10. For a good general discussion on this extremely important issue see, Zachary Goldman & Samuel Rascoff, GLOBAL INTELLIGENCE OVERSIGHT: GOVERNING SECURITY IN THE TWENTY-FIRST CENTURY (2016), in particular Part Two. The links between authorization and ongoing supervision, and ex-post facto review are discussed in Section III(C).

11. Examples include courts, parliamentary committees, watchdogs, and independent expert bodies. *See* EUR. UNION AGENCY FOR FUNDAMENTAL RTS., SURVEILLANCE BY INTELLIGENCE SERVICES: FUNDAMENTAL RIGHTS SAFEGUARDS AND REMEDIES IN THE EU, VOLUME II: FIELD PERSPECTIVES AND LEGAL UPDATE 63-72 (Oct. 20, 2017) [hereinafter FUNDAMENTAL RIGHTS], https://perma.cc/3ZJT-N96G.

12. *See*, *e.g.*, Big Brother Watch and Others v. the United Kingdom, App. Nos. 58170/13, 62322/14, & 24960/15, ¶ 309 (Sept. 13, 2018), https://perma.cc/VQH5-D2DW.

13. *See*, *e.g.*, *Big Brother Watch*, App. Nos. 58170/13, 62322/14, & 24960/15, ¶ 320.

14. This type of mechanism is, in principle, compatible with the oversight frameworks in place in a large number of jurisdictions, and so the discussion herein should be of broad relevance.

complement judge-led mechanisms, rather than when acting as the exclusive form of oversight.[15]

Section I discusses general factors relevant to ensuring that oversight is human rights compliant.[16] It examines the form that a human rights compliant body could take; the importance of ensuring adversarial "points of friction" to protect against unwarranted deference to security agencies; the necessity of maintaining a bright line distinction between the authorization and ongoing supervision stages, and of ensuring that both stages are sufficiently robust (that is, deficiencies at one stage are not tolerated, on the understanding that they are compensated for elsewhere). Section II analyzes the authorization process. It discusses the importance of authorization at both the collection and access to data stages, the margin of appreciation that may be permitted to the security services or the executive, and the scope of review. Section III then looks at the ongoing supervision of authorized surveillance activities. It addresses the resources necessary to ensure effective oversight, including technical expertise, and the need for longer term thematic review,[17] as well as any links between the oversight mechanism and the ex post facto review tribunal.

I. FACTORS RELEVANT TO ENSURING THAT OVERSIGHT MECHANISMS ARE HUMAN RIGHTS COMPLIANT

The ECtHR has noted that "it is in principle desirable"[18] to entrust surveillance oversight to a judge, in light of the perceived benefits associated with judicial control, such as independence, impartiality, and adherence to appropriate processes and procedures.[19] This section will address and develop these elements, looking at: whether a bulk surveillance oversight mechanism should be a court or a judge-led body; the independence requirement, including how independence can be ensured in practice; how the incorporation of points of friction within a body can facilitate impartiality and protect against "capture" or "case hardening" whereby, over time, oversight officials begin to identify with intelligence agencies thereby undermining their independence and oversight effectiveness; and how the separation of the authorization and ongoing supervision phases can

15. In particular, such bodies do not typically offer the judicial qualities that are a consistent feature of European Court of Human Rights case law and are unlikely to be able to satisfy the overall requirements of an oversight mechanism (including operating on a full-time basis) as discussed in Section I. These bodies do, however, play an important role, and can act as an essential complement to the type of oversight mechanism discussed in this article. For a discussion of other oversight mechanisms, see FUNDAMENTAL RIGHTS, *supra* note 11.

16. The focus is on the case law of the European Court of Human Rights, as this is the human rights court which has engaged most consistently and in detail with the issues under discussion.

17. Thematic review refers to the ability to review different categories of intelligence operations and as such forms part of the ongoing supervision of intelligence agency activities. As it is not concerned with investigating – and providing an effective remedy for – suspected violations it is distinct from the ex post facto review process, despite the fact that the operations themselves may have concluded.

18. *Big Brother Watch*, App. Nos. 58170/13, 62322/14, & 24960/15, ¶ 309.

19. Zakharov v. Russia, App. No. 47143/06, ¶ 233 (Dec. 4, 2015), https://perma.cc/7MK4-LKXD; *see also* Rotaru v. Romania, 2000-V Eur. Ct. H.R. 109, ¶ 59.

facilitate proper procedure. As noted above, the focus here is on the first two phases of the oversight process: authorization and ongoing supervision.

A. What Does Human Rights Law Say Vis-à-Vis the Type of Oversight Body?

To-date, ECtHR case law has indicated a clear preference that oversight be conducted by a judicial body, such as a court or tribunal. Since *Klass*, the first case to deal with large-scale surveillance, the Court has consistently stated that: "in a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge."[20] Underpinning this reasoning is the belief that "judicial control affords the best guarantees of independence, impartiality and a proper procedure."[21]

This requirement, however, is not absolute. In several cases, the ECtHR has held that, under appropriate conditions, non-judicial control or oversight may be compatible with the requirements of international human rights law. For instance, in *Zakharov,* the Court stated that, "although it is in principle desirable to entrust supervisory control to a judge, supervision by non-judicial bodies may be considered compatible with the Convention".[22] In *Big Brother Watch,* the Court was unequivocal, holding that judicial authorization was not a "necessary requirement" and that the exclusion of judicial control was not outside "the limits of what may be deemed necessary in a democratic society."[23]

This raises the possibility that a number of different types of oversight mechanism may be permissible, necessitating that questions be asked as to what is required to ensure effective oversight, and what bodies are capable of meeting these requirements. A number of factors have been identified as essential,[24] and a clear and consistent criterion emerging from the case law is that the body be able to "exercise an effective and continuous control."[25] This indicates that the oversight body should have appropriate powers to enable it to effectively assess all aspects of surveillance activity (necessitating sufficient subject-matter expertise), on an ongoing (continuous) basis.[26] The two elements will now be examined.

The act of surveillance is a dynamic, ongoing process, the specifics of which will inevitably evolve over the course of an operation. For instance, in a bulk

20. Klass v. Germany, 28 Eur. Ct. H.R. (ser. A) ¶ 56 (1978).
21. *Id.* ¶ 55; *Rotaru*, 2000-V, ¶ 59.
22. *Zakharov*, App. No. 47143/06, ¶ 275.
23. *Big Brother Watch*, App. Nos. 58170/13, 62322/14, & 24960/15, ¶ 318.
24. Other criteria are discussed further in Sections I(C) - (E).
25. *Zakharov*, App. No. 47143/06, ¶ 275.
26. Although the European Court has not provided explicit guidance as to what is required by "continuous" oversight, the authors interpret this as requiring ongoing, or full time, engagement. This is particularly necessarily in light of the oversight requirements established in *Big Brother Watch* which included, for example, oversight with respect to "the entire selection process, including the selection of bearers for interception, the selectors and search criteria for filtering intercepted communications, and the selection of material for examination by an analyst." *See Big Brother Watch*, App. Nos. 58170/13, 62322/14, & 24960/15, ¶ 387. Undertaking this level of supervision is arguably a full time task, as demonstrated, for instance, by the figures in footnote 27.

surveillance context the selectors used to access large data sets, and to produce more refined information for human analysis, may be modified. Given the scale of bulk surveillance, and the variable granularity of selectors, this could bring information relating to a significant number of individuals into play. This is distinguished from traditional targeted surveillance, whereby specific individuals or devices are subject to scrutiny. Exercising continuous control over bulk surveillance operations therefore requires significant resources,[27] and frequent engagement with the relevant agencies. Such day-to-day engagement with the practice of surveillance actors may include a number of different functions, such as spending time in intelligence or security agencies monitoring actual practices to understand how surveillance activities are carried out and their impacts, or 'digging' to follow live operations or uncover unusual behaviours. This task is most appropriately conducted by a full-time body: 'Full-time, ongoing oversight is particularly important for monitoring the legality of security service work because this tends to be complex, time-intensive and detailed work.'[28] Indeed, in the absence of a full-time body, it is difficult to see how 'continuous control' can be exercised given the scale of the task at hand.

To effectively control complex modern surveillance operations, specific subject-matter expertise is also appropriate. This necessitates at least two elements. First, in-depth engagement with the practice of surveillance, over time, will inevitably be necessary to develop appropriate expertise and understanding:

> Obviously, it takes a long time for any external monitoring body to penetrate the arcane world of intelligence, to understand what is a 'reliable' intelligence assessment, and why this is so. Unless and until they are in a position to make a reasonably informed 'second assessment', a monitoring body is not a real safeguard.[29]

Second, the complexity of the underlying technology and rapid developments in this area indicate that specific expertise is also necessary. This suggests that the oversight body should have the ability to employ a range of subject-matter experts.[30] For instance, understanding the underlying technical issues and the potential inherent in surveillance technology is clearly essential to understanding the legal and human rights impact: oversight officers must be able to understand the extent of information that can be revealed. Technical expertise is therefore

27. During a workshop hosted by the authors during March 2018 representatives from U.K. oversight bodies stated that they authorised around 12,000 applications for surveillance warrants each year and estimated this to be three times the caseload of FISA courts in the US. The scale of such activity raises obvious implications for resourcing, and so staffing, budget, etc. are all essential factors to address.

28. COUNCIL OF EUR. COMM'R FOR HUM. RTS., DEMOCRATIC AND EFFECTIVE OVERSIGHT OF NATIONAL SECURITY SERVICES 47 (2015) [hereinafter OVERSIGHT OF NATIONAL SECURITY SERVICES], https://perma.cc/H5P2-PHTX.

29. EUR. COMM'N FOR DEMOCRACY THROUGH L. (VENICE COMM'N), DEMOCRATIC OVERSIGHT OF THE SECURITY SERVICES ¶ 90 (2015) [hereinafter VENICE COMM'N], https://perma.cc/23RR-Y8ZJ.

30. *See* OVERSIGHT OF NATIONAL SECURITY SERVICES, *supra* note 28, at 14, 50.

relevant both to the assessment of surveillance authorization requests, and to the supervision of ongoing surveillance operations. Equally, engagement with the day-to-day practice of surveillance (such as the monitoring and 'digging' referred to above) is arguably best undertaken by dedicated inspectors or investigators with specialized knowledge and expertise, particularly in regard to intelligence 'tradecraft'.

Human rights case law accordingly suggests that, in order to complete its tasks as effectively as possible, an oversight body should operate continuously, and possess sufficient surveillance-focused expertise, including technical expertise. The question then, of course, is what kind of body can satisfy these requirements?

B. What Type of Oversight Body is Appropriate?

Traditional judicial bodies, such as courts or tribunals – at least in common law systems – are typically not set up in a manner amenable to satisfaction of the above criteria. Courts are primarily responsive entities, addressing specific issues or complaints as they are brought before them, and judges appointed to such bodies are typically not in a position to exercise continuous control over day-to-day surveillance activities.[31] As such, an oversight mechanism that can operate beyond the constraints associated with a court or tribunal – for instance, by engaging with surveillance authorities on a full-time, and proactive basis, and by employing a sufficient diversity of staff to ensure effective and continuous control – appears to offer significant benefits.[32]

However, a body without judicial characteristics or judicial review expertise does not seem appropriate.[33] As noted, the European Court has consistently stated that 'it is in principle desirable' that oversight be conducted by a judicial body, in light of the particular qualities that this brings.[34] As such, and in order to ensure the necessary judicial qualities,[35] experience, and knowledge of the system,[36] while avoiding the limitations associated with a court or tribunal, it is suggested that oversight mechanisms be judge-led, rather than 'just' an independent, technical body, for example.

---

31. Equally, it is not possible for the representatives of claimants to conduct such activities, as they will not have the required access.

32. Raphael Bitton, *In Law We Trust: The Israeli Case of Overseeing Intelligence*, *in* GLOBAL INTELLIGENCE OVERSIGHT: GOVERNING SECURITY IN THE TWENTY-FIRST CENTURY 141, 142 (Zachary K. Goldman & Samuel J. Rascoff eds., 2016).

33. Here, judicial characteristics are used to refer to the qualities typically associated with judges, as well as other factors, such as the ability to issue binding decisions. These are discussed further over the following paragraphs.

34. The status associated with judges and the implicit trust generated by their position are equally important factors.

35. These qualities may include knowledge of the law; experience conducting human rights analysis; institutional or political independence; the ability to analyze information and uncover facts; experience reviewing and challenging State activity; and an understanding of legal and procedural complexity.

36. *See* Rotaru v. Romania, 2000-V Eur. Ct. H.R. 109, ¶ 59; Klass v. Germany, 28 Eur. Ct. H.R. (ser. A) ¶ 55 (1978) (highlighting the importance attributed to judicial qualities).

Judicial officers could be drawn from current or former judges with experience dealing with the legality of government activities.[37] Such individuals contribute to institutional and working independence, discussed further below. They also bring qualities that are particularly important for functions such as analyzing surveillance measures against the requirement of necessity/strict necessity.[38] To ensure independent *control* over the actions of the intelligence and security services, and to ensure that the oversight function is not merely recommendatory but also effective, judicial officers must also have the authority to issue binding decisions.[39] An example of this binding authority in practice is the 'double-lock' system established under the Investigatory Powers Act 2016, whereby judicial commissioners are granted the authority to review, and more importantly to reject, decisions of the Secretary of State authorising surveillance.[40]

An oversight mechanism could therefore consist of a two-tiered body, led by judicial officers and supported by a dedicated non-judicial staff. This 'court-plus' model should be formally and functionally independent, able to deliver in respect to the judicial qualities discussed above, and to scrutinize relevant activities in light of legal and human rights requirements, while also having the ability to engage continuously and to employ an appropriate array of non-judicial subject-matter experts.

In *Big Brother Watch,* the ECtHR indicated that oversight authority should extend into actual operational practice. In the context of bulk surveillance this requires the authority to address "the entire selection process, including the selection of bearers for interception, the selectors and search criteria for filtering intercepted communications, and the selection of material for examination by an analyst".[41] To facilitate this form of in-depth engagement the supporting non-judicial staff should include investigators and inspectors – and individuals with appropriate technical expertise – who would play a particularly prominent role in relation to the supervision of ongoing surveillance operations, but who would also play a key role in keeping the judicial officers up-to-speed on actual

37. A key element in effective oversight is the ability to challenge state or intelligence agency decisions, often in relation to issues of national security with significant potential consequences, so experience in this area is a clear benefit. Of course, ensuring independence, particularly of former judges, will require additional institutional safeguards, which are discussed further in Section I(C).

38. *See, e.g.*, Szabó v. Hungary, App. No. 37138/14, ¶ 76 (Jan. 12, 2016), https://perma.cc/UZK6-EAQA.

39. The Belgian Commission on exceptional methods of surveillance is interesting in this regard; it is an "administrative commission comprised of three security-cleared magistrates (acting in a non-judicial capacity) appointed by the executive, which gives 'binding advice' to the security services when they apply to use 'exceptional measures' (including surveillance)." Gianclaudio Malgieri & Paul De Hert, *European Human Rights, Criminal Surveillance, and Intelligence Surveillance: Towards "Good Enough" Oversight, Preferably but Not Necessarily by Judges*, *in* THE CAMBRIDGE HANDBOOK OF SURVEILLANCE LAW 523 (David Gray & Stephen E. Henderson eds., 2017). See Zakharov v. Russia, App. No. 47173/06, ¶ 282, (Dec. 4, 2015), https://perma.cc/7MK4-LKXD, for a discussion on the binding nature of oversight.

40. *See, e.g.*, Investigatory Powers Act 2016, § 140 (UK), https://perma.cc/3MSK-2PT7.

41. Big Brother Watch v. United Kingdom, App. Nos. 58170/13, 62322/14, & 24960/15, ¶ 387 (Sept. 13, 2018), https://perma.cc/VQH5-D2DW.

surveillance practices, and developing trends. The provision of technical expertise may take several different forms, but irrespective of the model adopted it is essential that independence and impartiality be ensured.[42] A duty to report, and a duty to engage with the public, may also be essential to facilitate transparency and trust in the system, and to facilitate an appropriate level of public engagement and public scrutiny. Ensuring public awareness of the oversight body's work should be regarded as an important task, essential to public confidence in the oversight system.

A dedicated oversight body such as the one outlined here would develop institutional knowledge, expertise, and best practice, and share information in-house, thereby facilitating both the development of up-to-date expertise and a more in-depth understanding of intelligence agency practices. This is particularly important as it helps to protect against unwarranted deference to the intelligence and security agencies.[43] There are potentially significant consequences associated with denying surveillance authorization or shutting down a surveillance operation. In the absence of in-depth expertise, experience, and an understanding of operational realities, it is likely that an oversight body will err on the side of caution and grant surveillance requests,[44] rather than challenging them in the interests of human rights compliance. This potential for caution is emphasized in a national security context.[45] To withstand such pressures, independence, expertise, knowledge, and experience, as well as wider respect and legitimacy, are required. Such challenges are faced by judges who are required to judge the legality of governmental action on a day-to-day basis.

Support for this form of oversight body may be found in the case law. For instance, both the Court of Justice of the European Union (CJEU) and the ECtHR have held that oversight may be conducted "either by a court or by an independent administrative body."[46] The body proposed here – a "court-plus" model – is an amalgamation of these two types of entities, and is capable of satisfying the requirements established in relation to surveillance oversight.[47] In *Big Brother Watch,* the ECtHR accepted the role of IPCO, a body broadly similar to that proposed, in that it is formed of judicial officers supported by non-judicial staff.[48] It is not suggested, however, that IPCO be directly emulated, noting, for example, the issues discussed below in relation to the separation of authorization and review processes, and the conflict of interest that arises from "marking your own

42. Discussed further in Section I(C).

43. Discussed further in Section I(D).

44. *See* VENICE COMM'N, *supra* note 29, ¶ 218.

45. Counterterrorism operations provide an example in this regard.

46. Joined Cases C-203/15 & C-698/15, Tele2 Sverige AB v. Post-och telestyrelsen, Sec'y of State for the Home Dep't v. Watson, ECLI:EU:C:2016:970, ¶ 120 (Dec. 21, 2016); *Big Brother Watch*, App. Nos. 58170/13, 62322/14, & 24960/15, ¶ 318.

47. Such requirements include guarantees of independence, impartiality, and a proper procedure, which are discussed further in Sections I(C) - (E).

48. *Big Brother Watch*, App. Nos. 58170/13, 62322/14, & 24960/15, ¶ 387.

homework."[49] However, the Court expressed clear endorsement of this broad approach to oversight, and this is consistent with the court-plus model being proposed here.

It is important to reiterate that the form of oversight body discussed in this section is directed at the authorization and ongoing supervision stages, and not the post-facto review process, which should be undertaken by a court or tribunal, including following receipt of specific complaints. This provides an important judicial safeguard,[50] while also facilitating individuals' access to an effective remedy.[51]

C. Independence

Both the ECtHR and the CJEU have confirmed that the body established to oversee surveillance activities must be independent.[52] To this end, the oversight mechanism should be independent of both the executive and the intelligence and security services that it oversees.[53] In ensuring the appropriate institutional structure, several factors are relevant. For example, the European Fundamental Rights Agency has highlighted the following: whether the law explicitly establishes the body's independence; rules on conflict of interest; the authority entitled to appoint oversight officers; budgetary allocations; and fixed terms of office.[54]

In addition to institutional factors, the ability of an oversight mechanism to function independently in practice is essential. It has been suggested that operational independence may be enhanced if the oversight body is housed in a different location from the executive branch or security services, and if its supervisory mechanisms are kept separate and external from security services' structures.[55] Other means of securing operational independence are more complex, however, and the security vetting of individuals appointed to an oversight body provides an illustrative example in this regard.

As discussed in greater detail below, oversight officers require security clearance so that they can gain an in-depth understanding of surveillance activities,

---

49. *See* Section I(E).

50. Szabó v. Hungary, App. No. 37138/14, ¶ 77 (Jan. 12, 2016), https://perma.cc/UZK6-EAQA; *see also Big Brother Watch*, App. Nos. 58170/13, 62322/14, & 24960/15, ¶ 318.

51. *See, e.g.*, Convention for the Protection of Human Rights and Fundamental Freedoms art. 13, Nov. 4, 1950, E.T.S. No. 5., 213 U.N.T.S. 222; International Covenant on Civil and Political Rights art. 2(3), Dec. 16, 1966, 999 U.N.T.S. 171.

52. *See* Zakharov v. Russia, App. No. 47173/06, ¶ 258 (Dec. 4, 2015), https://perma.cc/7MK4-LKXD; Joined Cases C-203/15 & C-698/15, Tele2 Sverige AB v. Post-och telestyrelsen, Sec'y of State for the Home Dep't v. Watson, ECLI:EU:C:2016:970, ¶ 125 (Dec. 21, 2016).

53. *See* Martin Scheinin (Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism), *Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight*, at 8, U.N. Doc. A/HRC/14/46 (May 17, 2010); OVERSIGHT OF NATIONAL SECURITY SERVICES, *supra* note 28, at 12; Ashley Deeks, *An International Legal Framework for Surveillance*, 55 VA. J. INT'L L. 291, 361 (2015).

54. FUNDAMENTAL RIGHTS, *supra* note 11, at 74.

55. *Id.* Shortly after its establishment, the UK Investigatory Powers Commissioner's Office moved to a separate location outside the Home Office, where it had been temporarily housed.

engage with the day-to-day activities of the intelligence and security services, and "dig" for information. However, it is typically these same services that conduct the vetting necessary to obtain security clearance. This process is usually secretive and the reasoning underpinning a decision to refuse security clearance may not be released, potentially for reasons of national security. However, a lack of transparency in this regard may give rise to concerns about the oversight body's ability to operate independently in practice. For instance, it is important to ensure that an oversight body – and individual oversight officers – can subject the activities of the intelligence and security services to robust challenge, such that they are required to explain and justify their actions, and to modify or cease activities if appropriate. This process may be undermined if these same intelligence and security services can, in effect, vet the members of the oversight body. For example, individuals with experience contesting state activities, including state surveillance activities, may form an important part of an oversight team, as they may bring with them relevant professional experience, a different point of view, and a fresh perspective vis-à-vis otherwise accepted narratives. Indeed, the recruitment of individuals with different points of view – and potentially individuals with direct experience contesting state claims – may facilitate the development of points of friction throughout the oversight mechanism.[56] Investigative journalists, human rights or civil liberties lawyers, civil society activists, or human rights defenders are all potential examples. Yet it is these individuals that security services may be particularly wary of in light of their previous work, and perhaps their previous clients or contacts. Should security clearance be refused, this will inevitably raise concerns, and may impact the body's independence and ability to operate effectively. This was apparently the case in the United Kingdom, where security clearance for the appointed head of investigations at IPCO was denied. The individual was a human rights professional, with previous experience at well-known non-governmental organizations. His security clearance was reportedly denied on the basis of his "previous work and associations".[57]

Resolving issues to do with the withholding of information on the basis of national security considerations is notoriously complex, and the appropriate balance between sufficient transparency to ensure trust and sufficient secrecy of information essential to national security is difficult to strike. One possible way to resolve this issue is to require that negative security clearance decisions (as they pertain to oversight officers) be reviewed by the court or tribunal established to conduct the ex post facto review.[58] These judges will have an interest in the

56. Points of friction are discussed further in Section I(D).

57. Mark Townsend, *Home Office under fire for blocking new spy watchdog*, GUARDIAN (Jan. 19, 2019), https://perma.cc/P88J-857W.

58. In the United Kingdom, this would be the Investigatory Powers Tribunal. This would be an important additional safeguard, as a right of appeal may not be available to candidates for employment, who are not offered employment on the basis of rejected security clearance. This is the case, for

effective functioning of the oversight body, a familiarity with the work of the intelligence agencies, and a sensitivity to national security considerations.[59]

An additional issue that arises is how to recruit such individuals in the first instance. There may be a reluctance to work for an oversight body, as a result, for instance, of the concern that it may whitewash state activity. The ability of the oversight body to demonstrate its operational independence may be an important factor in this regard, underlining the importance of transparency. There is no set route to achieving increased trust in the work of an oversight body. One possibility may be to establish regular meetings between oversight/judicial officers and key civil society actors such as human rights organizations, lawyers active in the area, and national human rights commissions. These meetings could be held under the Chatham House rule, and may provide an opportunity for oversight officers to engage with, and develop relationships with, key external actors, and to hear from different perspectives. At one end of the continuum these meetings could address issues of general concern to civil society and provide a forum for different points of view to be raised. At a more focused level, the oversight body could prepare, and invite discussion around, hypothetical scenarios of relevance to their work.[60] Equally important are other factors such as strong recruitment drives and openness to recruit more broadly.

D. Points of Friction

A key concern associated with oversight bodies is that of "capture"[61] or "case hardening."[62] This is a phenomenon whereby, over time, oversight officers or specialized judges begin to identify with security officials,[63] thereby undermining, or potentially negating, their critical edge and independence. The potential for this phenomenon to emerge is clear. Due to the nature of surveillance oversight, and in particular the level of secrecy associated with national security considerations, oversight officers and specialized judicial bodies typically only engage with security officials. For instance, during the authorization and oversight phases, the individuals subject to surveillance are not informed of the fact of surveillance, and so are not in a position to defend their interests or otherwise inform the process. Instead, it is security officials who set out the case for

example, regarding the Security Vetting Appeals Panel in the United Kingdom. *See Security Vetting Appeals Panel*, GOV.UK, https://perma.cc/VS4F-URGG.

59. Importantly, in the model discussed in this paper, the ex post facto tribunal is completely distinct from the oversight body, and so independence and impartiality with respect to who may be appointed to an oversight body is maintained.

60. This element was a key success in workshops organized by the authors and gave rise to a number of markedly different opinions and approaches.

61. There is a rich literature on regulation discussing the problem of 'capture,' i.e situations where regulatory systems risk being 'captured' by those they are supposed to regulate. George Stigler, *Theory of Economic Regulation*, 2 THE BELL J. ECON. & MGMT. SCI., no. 1, (1971), at 3 cited by ROBERT BALDWIN, MARTIN CAVE & MARTIN LODGE, UNDERSTANDING REGULATION 43 (2d ed. 2012) ("[A]s a rule regulation is acquired by the and is designed and operated primarily for its benefit.").

62. VENICE COMM'N, *supra* note 29, ¶ 30.

63. *Id.*

surveillance, including the necessity of the measures, and potentially the risks associated with the failure to act. The nature of this process means that oversight officers consistently engage with only one perspective. An inability to engage with other perspectives will inevitably narrow the scope for critical engagement, undermining the efficacy of any oversight measure.[64] Protecting against capture/case hardening is therefore central to the nature and quality of the oversight process and the level of challenge the intelligence body receives. The Council of Europe Commissioner for Human Rights has noted that:

> experience shows that security agencies can develop a "State within a State" mentality. A culture of regarding any non-mainstream political movement as a threat to the State can emerge. [. . .] a problem for the personnel of any security agency is that they can develop a "security mindset". Improved democratic scrutiny is thus not simply to protect against abuse of human rights but also *to expose the intellectual assumptions and work practice of security personnel to informed criticism.*[65]

Facilitating diverse points of view, and mitigating the effects of case hardening, may be achieved by the incorporation of multiple "points of friction" into the oversight process. A "point of friction" is not a term of art.[66] Rather, it is a phrase intended to capture those points in the oversight process where critical adversarial voices may be introduced to challenge existing assumptions or practices, add different perspectives, and require the unpacking and critical examination of the reasoning underpinning different approaches. The necessity of ensuring some form of adversarial process was clearly indicated by the ECtHR in *Janoweic*:

> . . .even where national security is at stake, the concepts of lawfulness and the rule of law in a democratic society require that measures affecting fundamental human rights must be subject to some form of adversarial proceedings before an independent body competent to review the reasons for the decision and the relevant evidence. If there was no possibility of challenging effectively the executive's assertion that national security was at stake, the State authorities would be able to encroach arbitrarily on rights protected by the Convention.[67]

---

64. Such processes reflect a broader tendency towards 'asymmetric surveillance' recognised in the scholarship of advanced surveillance practices. Itself drawn from longstanding analyses of fiscal markets, and in particular the work of Nobel prize winning economist George Stigler's work on 'information asymmetries,' studies of asymmetric surveillance argue that such disparities are actively constructed, have multiple identifiable drivers (including specific forms of knowledge production and the particularities of legal and organisational structures, exclusive information network) and hold significant implications (including restrictions on access to justice, receding opportunities for transparency and the reproduction of social disadvantage). *See, e.g.*, George J. Stigler, *The Economics of Information*, 69 J. POL. ECON., no. 3, at 213 (1961); Geoffrey Lightfoot & Tomasz Piotr Wisniewski, *Information Asymmetry and Power in a Surveillance Society*, 24 INFO. & ORG. 214 (2014).

65. VENICE COMM'N, *supra* note 29, ¶ 61.

66. The term was first introduced to the authors of this paper by Ben Wizner.

67. Janowiec v. Russia, 2013-V Eur. Ct. H.R. 203, 275.

Points of friction may be introduced at multiple stages throughout the surveillance oversight process. Two examples are given here for illustrative purposes. First, points of friction may be incorporated directly into the oversight body itself by hiring staff from diverse backgrounds.[68] Diversity among staff can help to avoid the emergence of stereotypes or "baked in" discrimination, and their perspective could also help to ensure the presence of critical voices within the oversight body.[69] Such individuals' experience may make them particularly suited to roles such as legal analysis, the direct monitoring of surveillance activity (including "digging" to investigate operational practice and uncover any irregularities), or longer-term thematic review.

Second, security-cleared special advocates could be introduced to represent the individual and societal interests affected by surveillance practices, at a minimum during the authorization and ex post facto review stages.[70] At the authorization stage special advocates could potentially provide an important third-party point of friction, capable of informing the oversight body's review, and militating against any potential capture/case hardening on the part of the oversight body/officer. As noted by the ECtHR in relation to individuals directly affected:

> [T]he very nature and logic of secret surveillance dictate that not only the surveillance itself but also the accompanying review should be effected without the individual's knowledge. Consequently, since the individual will necessarily be prevented from seeking an effective remedy of his own accord or from taking a direct part in any review proceedings, it is essential that the procedures established should themselves provide adequate and equivalent guarantees safeguarding the individual's rights.[71]

Variations of the special advocate role are in place in a number of jurisdictions, including the United Kingdom and Canada.[72] In relation to Canada, for example, it has been claimed that "security-cleared amicus who had access to relevant classified information [. . .] can be helpful to the extent that they can serve an adversarial challenge function."[73] Incorporation of this type of role was also an explicit recommendation of the Council of Europe Commissioner for Human Rights:

---

68. *See* discussion on potential candidates *supra* Section I(C).

69. The phenomenon of discriminatory outcomes resulting due to a lack of diversity among decision-makers has been reflected in analogous contexts in the criminal justice system. For example, socio-legal research has consistently pointed to the disadvantage in sentencing decisions experienced by ethnic minorities and those from poorer backgrounds when facing white judges of higher socio-economic class. *E.g.,* ROGER HOOD, RACE AND SENTENCING (1992); ANDREW ASHWORTH, SENTENCING AND CRIMINAL JUSTICE (2012).

70. Given the equally applicable possibility of capture, case hardening issues related to recruitment of suitable candidates and security clearance are equally relevant here. See discussion *supra* Section I(C).

71. Klass v. Germany, 28 Eur. Ct. H.R. (ser. A) ¶ 55 (1978).

72. *See, e.g.*, ANNUAL REPORT OF THE INVESTIGATORY POWERS COMMISSIONER 2017, INVESTIGATORY POWERS COMMISSIONER'S OFFICE 10 (2017).

73. Kent Roach, *Review and Oversight of Intelligence in Canada: Expanding Accountability Gaps, in* GLOBAL INTELLIGENCE OVERSIGHT: GOVERNING SECURITY IN THE TWENTY-FIRST CENTURY 191 (Zachary K. Goldman & Samuel J. Rascoff eds., 2016).

> Consider the introduction of security-cleared public interest advocates into surveillance authorization processes, including both targeted and untargeted surveillance measures, to represent the interests of would-be targets of surveillance.[74]

It should be noted that the role of special advocates is not without controversy, particularly with respect to judicial proceedings involving the right to liberty or the right to a fair trial.[75] Any measures adopted should ensure a genuine adversarial process whereby the nature of the government's claims can be effectively challenged. Efforts must also be made to ensure that the pool of special advocates is diverse, incorporating individuals who have also acted against the government.[76] In this context, the issues raised in Section I(C) regarding the security clearance process are likely to resurface.

An important concern is that of transparency with respect to making processes available for public scrutiny. Bringing a "civic voice" into oversight decision-making and, additionally, affording a measure of public scrutiny to oversight decisions are crucial components of this process: transparency should be the rule, and secrecy the exception. While the secretive nature of intelligence activities poses certain problems for such an approach it does not follow, for instance, that information *about* decisions must be subject to the same restrictions. For example, possibilities exist for oversight bodies to publish the number of decisions they declined ownership of and left to the internal processes of particular intelligence agencies. Equally, the onus should be on the intelligence agencies to set out why information should be restricted, to ensure that transparency rather than secrecy is the rule.

E. The Separation of Authorization and Supervision Functions

To define the precise features of human rights compliant oversight it is important to delineate its core functions. This is something underdeveloped in current critical scholarship on intelligence oversight, a gap this paper seeks to address. As discussed above, this article separates oversight into three phases: the authorization phase, the ongoing supervision of surveillance activities phase, and the post-facto review phase. This article focuses on the first two of these phases, namely authorization and ongoing supervision. Two questions arise regarding the relationship between these phases. First, whether the same body should be

---

74. OVERSIGHT OF NATIONAL SECURITY SERVICES, *supra* note 28, at 12.

75. *See* JUSTICE AND SECURITY GREEN PAPER: RESPONSE TO CONSULTATION FROM SPECIAL ADVOCATES (2011), https://perma.cc/89MU-8KFC (presenting the majority of U.K. special advocates, who raise a number of significant concerns)*; see also* John Jackson, *The Role of Special Advocates: Advocacy, Due Process and the Adversarial Tradition*, 20 INT'L J. EVIDENCE & PROOF 343 (2016); Aileen Kavanagh, *Special Advocates, Control Orders and the Right to a Fair Trial,* 73 MOD. L. REV. 836 (2010); Graham Hudson & Daniel Alati, *Behind Closed Doors: Secret Law and the Special Advocate System in Canada,* 44 QUEEN'S L.J. 1 (2018).

76. *See* Hudson & Alati, *supra* note 75, at 39 (relating to concerns raised regarding the perceived independence of special advocates).

involved in both phases. Second, whether the phases should be regarded as interdependent such that shortcomings in one phase may be offset by enhanced scrutiny in the other. These two elements will be addressed in turn.

In a number of contexts – such as the United Kingdom – the same body conducts oversight of both the authorization and the ongoing supervision phases. There are merits to this approach, as it allows for the development of in-depth expertise within an oversight body, and for associated benefits related to information sharing, improved understanding of surveillance practices, and so on. However, some participants in an expert meeting organized as part of the Human Rights, Big Data & Technology Project criticized this approach on the basis that the oversight body is asked to, in effect, "mark its own homework,"[77] with potential implications for the effectiveness of the second phase review due to 'an inherent risk of a conflict of interest arising.[78] Protecting against "marking your own homework" was regarded as particularly important in the Canadian inquiry into the circumstances surrounding the rendition and subsequent torture of Mohammed Arar, which implicated the actions of the intelligence and security agencies. The inquiry "stressed the importance of reviewer independence from the activities that they review, so that reviewers are not co-opted by having given prior approval to national security activities that have failed or had unintended effects."[79]

There is clear potential for an actual or perceived conflict of interest to arise should these two oversight phases be combined. To protect both the effectiveness of the review process, and external perceptions of its effectiveness, the two roles should arguably be kept distinct, and a bright line distinction drawn between the authorization and ongoing supervision phases. However, the question arises as to whether an institutional firewall will satisfy these requirements, such that a separation of these roles does not necessarily require the establishment of two oversight bodies. The authorization and review processes could be kept distinct within the same body, for instance through the establishment of distinct departments, staffed by dedicated personnel, and with an institutional framework in place capable of ensuring their independence. While there may be risks that this approach would not secure absolute confidence in the process, it is arguable that

77. This was raised by a number of civil society representatives during workshops organized by the Human Rights, Big Data & Technology Project and the Investigatory Powers Commissioner's Office. *See generally* THE HUMAN RIGHTS, BIG DATA AND TECHNOLOGY PROJECT, https://perma.cc/P4ZW-KRM2.

78. OVERSIGHT OF NATIONAL SECURITY SERVICES, *supra* note 28, at 43. It is also important to note a defense to the 'marking your own homework' argument made by oversight agencies. In a workshop convened by the authors (Landmark Chamber, London, 14 March 2018) representatives from a U.K. oversight agency argued that combining the authorization and review stages conferred several advantages. These included the claims that oversight judges have sight of all applications rather than just a sample, which would be the case for other oversight procedures; opportunities exist to refine the approvals approach and hone questions based on learning from review work; it enables inspection team to directly refuse warrants; and, ultimately, inspection regime recommendations can be imported directly into practice.

79. Roach, *supra* note 73, at 180.

it may be capable of seizing the benefits associated with a single oversight body in terms of increased understanding of the intricacies of surveillance practice – for instance, internal briefings could be put in place to address all aspects of the surveillance process, challenges faced, best practices, and so on – while at the same time preventing a conflict of interest. Of course, issues of confidence in the process are paramount, and so further consideration should be given as to whether a single firewalled oversight mechanism, or two distinct mechanisms, is most appropriate.

The relationship between the authorization and ongoing supervision phases, in terms of the overall effectiveness of oversight, must also be addressed. ECtHR case law has tended to regard both phases as interdependent. On this understanding, deficiencies in one phase may be remedied by more stringent requirements in the other phase, thereby – it is believed – ensuring *overall* oversight effectiveness. This has been most frequently addressed in the context of judicial authorization of surveillance measures.[80] For instance, in *Centrum for Rättvisa*, the Court held that:

> . . . the rule of law implies, *inter alia*, that an interference by the executive authorities with an individual's rights should be subject to an effective control which should normally be assured by the judiciary, at least in the last resort, judicial control normally offering the best guarantees of independence, impartiality and a proper procedure [. . .] Prior judicial authorisation may serve to limit the authorities' discretion in interpreting the scope of mandating and performing signals intelligence. Thus, a requirement of prior judicial authorisation constitutes an important safeguard against arbitrariness [. . .] Nevertheless, prior authorisation of such measures is not an absolute requirement *per se*, because where there is extensive subsequent judicial oversight, *this may counterbalance the shortcomings of the authorisation*.[81]

If mass surveillance is examined solely through a right to privacy lens, and is focused exclusively on the harm to affected individuals rather than broader societal impacts, then the Court's approach may appear reasonable: subsequent review can facilitate the provision of an effective remedy, thereby addressing the individual harm. This approach, however, risks downplaying the harm caused by inappropriate authorizations and the difficulty of providing a fully effective remedy at the post-facto review stage. Of relevance here are the potentially significant number of individuals involved, the potentially invasive nature of the information, and the variety of uses to which information can be put (that is information obtained by surveillance may be fed into other decision-making processes, informing future decisions). This approach also fails to take into account

80. Szabó v. Hungary, App. No. 37138/14, ¶ 77 (Jan. 12, 2016), https://perma.cc/UZK6-EAQA.

81. Centrum for Rättvisa v. Sweden, App. No. 35252/08, ¶ 133 (June 19, 2018) (emphasis added), https://perma.cc/C3NV-48QM.

the broader societal effects of surveillance, and in particular the existence of a "chilling effect."[82]

The chilling effect is a phenomenon associated with surveillance activity whereby individuals refrain from engaging in certain lawful conduct because they are afraid of the consequences that may arise should such conduct be observed;[83] this is particularly relevant in the context of bulk surveillance given the large-scale nature of the practice. The chilling effect directly brings into play the right to privacy, as it is the monitoring of certain activity that gives rise to a chill. However, the human rights impacts are much broader. The rights to freedom of opinion, freedom of expression, freedom of association, freedom of assembly, and freedom of thought, conscience, and religion are all directly affected. Importantly, the effects in this area may be cumulative and not just felt at an individual level. It is the effect on privacy, opinion, expression, association, assembly, thought, conscience, and religion as inter-dependent rights with society-wide implications that is at issue. The harm cannot be considered fully by analyzing these rights in isolation, as it is the combination of the rights that serve to protect and facilitate the functioning of democracy. An exclusive privacy focus is therefore inappropriately narrow and is incapable of taking into account the overall human rights impact.

Importantly, a chilling effect arises not only when consequences actually follow should certain activity be observed, but also when it is feared that such consequences may follow. In this regard, it is the fear of surveillance, and uncertainty as to surveillance practices, that is decisive.[84] Rigorous scrutiny of the authorization process is therefore essential, as it is precisely at this point that large-scale surveillance is initiated and a possible chilling effect may begin to emerge. The nature of a chilling effect means that its impacts cannot be mitigated by subsequent review as it is the very fear of surveillance that is at issue. As such, effective authorization phase protections are essential, in and of themselves. In light of the broad harms associated with large-scale surveillance, it is imperative that the authorization and ongoing supervision phases be treated as entirely distinct from an oversight perspective, with each evaluated on its merits. Simply put, damage may be done at the authorization stage that cannot later be fully remedied.

82. For more in-depth discussion on, see Daragh Murray & Pete Fussey, *Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data*, 52 ISR. L. REV. 31 (2019) (discussing the chilling effect as applied to large scale surveillance).

83. *See, e.g.*, Valerie Aston, *State Surveillance of Protest and the Rights to Privacy and Freedom of Assembly: A Comparison of Judicial and Protester Perspectives,* 8 EUR. J. L. & TECH. 1, 2 (2017); Joe Purshouse & Liz Campbell, *Privacy, Crime Control and Police Use of Automated Facial Recognition Technology*, 17 CRIM. L. REV. 188, 196 (2019).

84. *See* Klass v. Germany, 28 Eur. Ct. H.R. (ser. A) ¶ 41 (1978) (relating to the finding of the European Court of Human Rights regarding the 'menace of surveillance').

II. THE AUTHORIZATION PHASE

This section focuses on issues relevant to the authorization phase, looking at the scope of authorization review, the factors required to conduct an effective review, and issues arising in relation to any potential "margin of appreciation."

A. The Scope of Authorization Review: Collection and Access

The European Union Fundamental Rights Agency has noted that it is precisely at the surveillance authorization stage that "safeguards on general surveillance of communications operations are most relevant."[85] To ensure that safeguards are effective, the authorization process should regulate both the collection or retention of data, *and* all subsequent access to that data. Indeed, inadequate controls on access will negate any collection/retention safeguards and fundamentally alter the "necessity" evaluation.

Strict access controls are particularly important in the context of bulk or large-scale surveillance to mitigate harm, and to limit the extent of any potential chilling effect. For instance, if it is known that access to surveillance data is tightly circumscribed and limited, for example to activity necessary in relation to a narrowly defined set of circumstances, such as those involving foreign-based terrorist organizations, it is possible that the resultant chilling effect may be limited. It is precisely when surveillance impacts on individuals and organizations, and in particular those situated in opposition to the prevailing status quo, that a chill is likely to be experienced. Accordingly, if a chill is to be mitigated, it appears necessary that a bright line ring fencing of surveillance data be maintained. An authorization review by an effective oversight body is essential in this regard. This requirement has been confirmed in the case law. In *Tele2/Watson* the CJEU held, in relation to authorization, that: "it is essential that access of the competent national authorities to retained data should, as a general rule [. . .] be subject to a prior review carried out either by a court or an independent administrative body."[86] In *Big Brother Watch,* the ECtHR required that authorization control examine all aspects relating to data access, including "the search criteria and selectors used to filter intercepted communications."[87]

In certain emergency situations, prior authorization may not be feasible. The case law recognizes this possibility – and its exceptional nature – holding that prior authorization is required, except in situations of "validly established urgency."[88] However, to protect against abuse it appears appropriate that both those situations qualifying as an emergency, and the scope of any permissible access, be clearly defined in law and subject to operational guidance. The classification

85. FUNDAMENTAL RIGHTS, *supra* note 11, at 93.

86. Joined Cases C-203/15 & C-698/15, Tele2 Sverige AB v. Post-och telestyrelsen, Sec'y of State for the Home Dep't v. Watson, ECLI:EU:C:2016:970, ¶ 125 (Dec. 21, 2016).

87. *Big Brother Watch*, App. Nos. 58170/13, 62322/14, & 24960/15, ¶ 340.

88. *Joined Cases*, ECLI:EU:C:2016:970, ¶ 120.

of a situation as an emergency, and the associated decision that prior authorization was not possible, should itself also be the subject of review.[89]

B. Conducting an Effective Authorization Review

At the authorization phase the oversight body must evaluate any proposed surveillance activity based on the necessity, or strict necessity, test.[90] This requires an in-depth and rigorous review of the case for the initiation of surveillance, or for access to the product of surveillance. The requesting agency must therefore set out in detail factors such as the need for the measures requested and their potential impact. The case law provides indications as to what is required in this regard. Factors highlighted by the ECtHR in *Centrum for Rättvisa* include a requirement that surveillance applications "must specify not only the mission request in question and the need for the intelligence sought but also the signal carriers to which access is needed and the search terms – or at least the categories of search terms – that will be used."[91] In *Szabó ,* the Court noted the importance of providing supporting materials, and "in particular, a sufficient factual basis for the application of secret intelligence gathering measures which would enable the evaluation of necessity of the proposed measure."[92] This has been reflected in the recommendations of the Council of Europe Commissioner for Human Rights:

> Guarantee that all bodies responsible for overseeing security services have access to all information, regardless of its level of classification, which they deem to be relevant to the fulfilment of their mandates. Access to information by oversight bodies should be enshrined in law and supported by recourse to investigative powers and tools which ensure such access. Any attempts to restrict oversight bodies' access to classified information should be prohibited and subject to sanction where appropriate.[93]

A failure on the part of the intelligence/security agencies to provide reasons for surveillance renders it impossible to evaluate the necessity of the measures in question.[94] Equally important in this regard is some form of human rights risk or impact assessment. Impact or risk assessments (a form of due diligence) are not an explicit requirement of human rights law. However, they are a key means by

89. A number of factors are relevant in this regard, including: a) there must be a recorded and clear decision that there is an emergency; b) the factors and supporting evidence should be recorded; c) an ex post facto review of the 'emergency' decision and evidence should occur (if need be in closed proceedings); and d) the reviewing body should be guided ideally against adopting an unduly deferential approach.

90. Zakharov v. Russia, App. No. 47143/06, ¶ 232 (Dec. 4, 2015), https://perma.cc/7MK4-LKXD; Szabó v. Hungary, App. No. 37138/14, ¶ 57 (Jan. 12, 2016), https://perma.cc/UZK6-EAQA.

91. Centrum for Rättvisa v. Sweden, App. No. 35252/08, ¶ 139 (June 19, 2018), https://perma.cc/C3NV-48QM.

92. *Szabó*, App. No. 37138/14, ¶ 71.

93. OVERSIGHT OF NATIONAL SECURITY SERVICES, *supra* note 28, at 13.

94. *Szabó*, App. No. 37138/14, ¶ 71.

which (a) the obligation to respect human rights,[95] and (b) the requirement to ensure that any rights interference is necessary in a democratic society, can be fulfilled.[96]

The precise requirements associated with surveillance applications remain to be determined. However, it is clear that it is for the state to demonstrate the necessity of surveillance powers, and to detail why traditional alternatives are inadequate.[97] It is perhaps appropriate that state agencies "develop a methodology for ascertaining the degree of indispensability of bulk powers in any given application. The existence, operation and credibility of this methodology could be a key focal point for oversight agencies."[98]

In overseeing the authorization process, it is essential that the analysis conducted by the oversight body extend beyond an examination of the impact on the right to privacy. As noted above in the discussion on the chilling effect, an exclusively privacy-focused lens is incapable of addressing the totality of the potential harm. Large-scale surveillance is of a nature to threaten the effective functioning of democratic society.[99] As such, the impact of surveillance must incorporate an examination of all those rights central to the functioning of democratic society. The rights to freedom of opinion, expression, association, assembly, thought, conscience, and religion are directly brought into play, as is the prohibition of discrimination. It is important that any evaluation of the impact on these rights evaluate not only the impact vis-à-vis distinct rights, but also incorporate an analysis of the interconnected nature of the rights and how they protect both individual and societal rights.

C. Margin of Appreciation

A final element to address in this section is the potential existence of a "margin of appreciation," whereby an oversight body regards certain decisions as falling primarily within the executive or security agencies' competence, and accordingly grants a degree of deference in those areas. In practice, an oversight body's decision to grant a margin of appreciation will result in a less rigorous review in that area, and the question therefore arises as to the circumstances under which such a margin may be permissible.

---

95. Convention for the Protection of Human Rights and Fundamental Freedoms art. 1, Nov. 4, 1950, E.T.S. No. 5., 213 U.N.T.S. 222. The obligation to respect requires, *inter alia*, that states (or public authorities) not take any measures that directly violate human rights. To ensure respect for rights, some form of impact assessment is therefore required.

96. For more detailed discussion see, Hum. Rts. Council, Report of the Office of the UN High Commissioner for Human Rights on 'The Role of Prevention in the Promotion and Protection of Human Rights', UN Doc. A/HRC/30/20 paras. 7-9 (2015). *See also* SURVEILLANCE CAMERA COMM'R, FACING THE CAMERA: GOOD PRACTICE AND GUIDANCE FOR THE POLICE USE OF OVERT SURVEILLANCE CAMERA SYSTEMS INCORPORATING FACIAL RECOGNITION TECHNOLOGY TO LOCATE PERSONS ON A WATCHLIST, IN PUBLIC PLACES IN ENGLAND & WALES 12 (2020).

97. *See* Zakharov v. Russia, App. No. 47143/06, ¶ 232 (Dec. 4, 2015), https://perma.cc/7MK4-LKXD.

98. Murray & Fussey, *supra* note 82, at 31, 58.

99. *See*, *e.g.*, *Zakharov*, App. No. 47143/06, ¶ 232.

The U.K. Investigatory Powers Commissioner's Office provides an example of an oversight body reading a "margin of appreciation" into their role. Advisory Note 1/2018, which sets out the general approach taken by the oversight body in approving warrants, authorizations and notices, states that: "Judicial Commissioners will afford a very wide margin of judgment to the Secretary of State' in determining such matters" (that is, what counts as legitimate ways to achieve foreign policy or national security priorities. [100]

Unquestionably, certain issues regarding foreign policy and national security appropriately fall within the remit of the executive branch, in this instance the Secretary of State. This is the case, for example, in relation to the identification and prioritization of national security or foreign policy objectives. However, this must be distinguished from other factors which are regulated by international human rights law and which must accordingly be subject to effective oversight. Examples in this regard include the identification of particular activities that constitute a threat to national security, thereby justifying the use of bulk powers, or the means by which national security objectives should be pursued. These elements are clearly regulated by international human rights law and are subject to the necessity/strict necessity test. For instance, case law has consistently held that the use of bulk powers may only be regarded as necessary in a democratic society in relation to limited factors, such as the prevention of "serious crime."[101] In approving a warrant in relation to a particular type of threat or activity, the oversight body must therefore analyze and evaluate the warrant and supporting documentation, and then conduct a necessity analysis to determine whether, amongst other factors, the activity in question is necessary for the specified purposes, and whether the underlying objective qualifies as a serious crime. If discretion as to this determination is granted to the executive it would fundamentally undermine the oversight body's essential independent authorization and oversight function.[102] As domestic oversight bodies are tasked with ensuring "adequate and effective guarantees against abuse,"[103] it is imperative that they do not permit a margin of appreciation in relation to issues addressed by international human rights law, as this would inappropriately put such matters outside the scope of review.

The importance of a full and effective review of the relevant powers at a domestic level is underlined by the nature of a human rights law review at the regional level, particularly in Europe. The ECtHR has also developed a "margin of appreciation" doctrine to accommodate often significant differences among States' parties, while at the same time ensuring appropriate supervision. It was

100. INVESTIGATORY POWERS COMM'RS'S OFF., *Advisory Notice* 1/2018 ¶ 25 (Mar. 2018), https://perma.cc/WS5F-EW9G.

101. Joined Cases C-203/15 & C-698/15, Tele2 Sverige AB v. Post-och telestyrelsen, Sec'y of State for the Home Dep't v. Watson, ECLI:EU:C:2016:970, ¶ 120 (Dec. 21, 2016).

102. Centrum for Rättvisa v. Sweden, App. No. 35252/08, ¶ 119 (June 19, 2018), https://perma.cc/C3NV-48QM.

103. *Zakharov*, App. No. 47143/06, ¶ 232.

explained for the first time in *Handyside v. United Kingdom*, in the context of public morals, but has also been applied to state surveillance activity:[104]

> By reason of their direct and continuous contact with the vital forces of their countries, State authorities are in principle in a better position than the international judge to give an opinion on the exact content of these requirements as well as on the "necessity" of a "restriction" or "penalty" intended to meet them [. . .] Nevertheless, it is for the national authorities to make the initial assessment of the reality of the pressing social need implied by the notion of "necessity" in this context. Consequently, Article 10 para. 2 (art. 10-2) leaves to the Contracting States a margin of appreciation. This margin is given both to the domestic legislator ("prescribed by law") and to the bodies, judicial amongst others, that are called upon to interpret and apply the laws in force [. . .]
>
> Nevertheless, Article 10 para. 2 (art. 10-2) does not give the Contracting States an unlimited power of appreciation. The Court, which, with the Commission, is responsible for ensuring the observance of those States' engagements (Article 19) (art. 19), is empowered to give the final ruling on whether a "restriction" or "penalty" is reconcilable with freedom of expression as protected by Article 10 (art. 10). The domestic margin of appreciation thus goes hand in hand with a European supervision. Such supervision concerns both the aim of the measure challenged and its "necessity"; it covers not only the basic legislation but also the decision applying it, even one given by an independent court.[105]

Evidently, the margin of appreciation developed by the ECtHR is predicated on the existence of appropriate scrutiny at the domestic level. The European Court's margin of appreciation in effect grants a degree of deference to domestic authorities to accommodate different approaches. It is not intended to exclude certain areas from any form of human rights scrutiny. As such, to be effective, the European margin of appreciation is wholly dependent on the existence of rigorous oversight at the domestic level.

III. THE ONGOING SUPERVISION PHASE

A number of factors relevant to the "ongoing supervision" phase of oversight have been discussed above, in Section I. This section focuses on those factors relevant to an oversight body's ability to conduct effective oversight: the issues of access, adequate resources, and the links to ex post-facto review will be discussed in turn.

A. Access

A discussion regarding an oversight body's "access" typically focuses on two components: access to materials, and access to the agencies themselves. The

104. *Big Brother Watch*, App. Nos. 58170/13, 62322/14, & 24960/15, ¶ 314.

105. Handyside v. United Kingdom, App. No. 5493/72, ¶¶ 48-49 (Dec. 7, 1976), https://perma.cc/3WY4-KXVA.

requirement that oversight bodies possess the authority to access all relevant materials is clearly established in the case law. As stated by the ECtHR in *Centrum for Rättvisa*:

> As regards the supervisory body's powers and competences, it is essential that it has access to all relevant documents, including closed materials, and that all those involved in interception materials have a duty to disclose to it any material required.[106]

To facilitate effective oversight in this regard, the agencies themselves must develop internal procedures and protocols to ensure that surveillance activities are documented and recorded in an understandable manner, capable of being subject to external audit.[107] For example, in terms of providing an overview of surveillance activity, in Germany the following details must be disclosed to the Bundestag Control Panel every six months: "a list including the implementation of surveillance measures, requests for information to private companies, Schengen alerts entered into the police information system and personal data sent to foreign entities."[108]

Facilitating access necessarily requires that oversight personnel are granted security clearance, so that they can fully review all materials. However, access is not just about the ability to obtain specific documents, it is also about understanding the operation of the overall surveillance architecture, and so access to the agencies themselves is necessary. Oversight personnel must have the authority to monitor actual surveillance operations, to interview agency personnel, and to examine how different internal processes and protocols work in practice. Oversight personnel should also have the ability to initiate their own investigations,[109] and to "dig" into the agencies' practice. This is important, both to facilitating oversight in relation to a random sample of agency activity, and to developing a detailed understanding of practice so that anomalies or unusual activity can be spotted and followed up on. As noted above, this depth of engagement and understanding as to how surveillance is conducted – including insight into utility and harm – is essential if an oversight body is to operate effectively in practice. Otherwise, the risk of deference, and the possibility that security agency activity is accepted at face value, is too high. These factors are reflected in the best practice identified by the UN Special Rapporteur on Counter-terrorism:

> Oversight institutions enjoy specific powers to enable them to perform their functions. In particular, they have the power to initiate their own investigations

106. *Rättvisa*, App. No. 35252/08, ¶ 155.

107. The development of a human rights compliant internal culture within intelligence and security agencies is key. *See* OVERSIGHT OF NATIONAL SECURITY SERVICES, *supra* note 28, at 8; Scheinin, *supra* note 53, at 16.

108. OVERSIGHT OF NATIONAL SECURITY SERVICES, *supra* note 28, at 44.

109. FUNDAMENTAL RIGHTS, *supra* note 11, at 78.

> into areas of the intelligence service's work that fall under their mandates, and are granted access to all information necessary to do so. These powers of access to information encompass the legal authority to view all relevant files and documents, inspect the premises of intelligence services, and to summon any member of the intelligence services to give evidence under oath.[110]

B. Adequate Resources, Including Technical Expertise

The issues of access and adequate resourcing are interdependent. Sufficient resources should be available to the oversight body so that it can capitalize on the level of access granted. As discussed above, oversight is a resource intensive task that requires persistent, long-term engagement. Key in this regard is staffing, and in particular the availability of a sufficiently large pool of trained staff, with appropriate subject matter expertise.[111] Oversight bodies are typically staffed predominantly by lawyers. While lawyers must play an essential role within an oversight mechanism, there are a large number of different – and equally important roles – including, for example, dedicated inspectors, specialist investigators, and technical experts. It is the combination of these different roles that enable an oversight body to engage effectively with its mandate, and to address all areas of surveillance activity. In a study on surveillance oversight, the European Union Fundamental Rights Agency, noted that: "[w]ith oversight bodies largely staffed by legal specialists, the inability to [. . . effectively capitalize on access, and thus to conduct effective oversight] sometimes boils down to limited technical capabilities."[112] The UN Special Rapporteur on Privacy also picked up on the staffing issue – vis-à-vis both numbers and expertise – in his end of mission statement to the United Kingdom:

> The IPCO [Investigatory Powers Commissioners' Office] started its operation in September 2017 and would appear to be on track to be significantly better resourced than the combined strength of the authorities that it replaces. This does not detract however from the need to ensure that it is quickly and sufficiently resourced to enable it to be pro-active in its audit functions especially with a capacity to carry out technology audits at source-code level. Given a current complement of approx. 50 staff, I would recommend considering expansion by at least 30 additional staff including a strong contingent of technologically competent individuals able and willing to "get their hands dirty" with the nitty-gritty of checking systems deployed by intelligence services and law enforcement agencies.

110. Scheinin, *supra* note 53, at 9.
111. OVERSIGHT OF NATIONAL SECURITY SERVICES, *supra* note 28, at 50.
112. FUNDAMENTAL RIGHTS, *supra* note 11, at 9.

C. Links to Ex Post Facto Remedy

Links between the ongoing supervision process and the ex post facto review (conducted by an independent court or tribunal) should be established to ensure the effective protection of human rights. For instance, if the oversight body uncovers inappropriate or potentially illegal conduct during the ongoing supervision phase, an effective remedy must be pursued. This involves at least two elements. First, the process itself should be modified to ensure that similar problems do not arise in the future. Second, individuals' right to an effective remedy should be ensured. The public interest in ensuring compliance with human rights should also be protected by enabling challenges by NGOs and appropriate agencies such as domestic human rights bodies.[113] The specific means by which this is achieved will inevitably have to be determined on a case-by-case basis – in light of factors such as the existence of ongoing surveillance operations involving national security considerations – but it may require that the oversight body prepare a dossier to be transmitted to the ex post facto review tribunal for further investigation and adjudication. The possibility that the operation of the oversight mechanism, at either the authorization or ongoing supervision phases, be subject to judicial scrutiny should also be raised.

CONCLUSION

For large-scale surveillance activity to be regarded as human rights compliant in certain circumstances, it is essential that associated oversight mechanisms are able to operate independently and effectively. These mechanisms have an essential role to play if human rights compliance is to be ensured and abuse prevented. Importantly, they play a central role in ensuring confidence in the system. To date, however, relatively little human rights focused guidance addressing how oversight mechanisms should be established and how they should operate exists. This article sets out some of the key considerations relevant in this regard. In particular, it suggests that a human rights compliant oversight mechanism could consist of a two-tiered body, led by judicial officers and supported by a dedicated non-judicial staff. This "court-plus" model should be formally and functionally independent; such a model should deliver in respect to the judicial qualities discussed above and scrutinize relevant activities in light of legal and human rights requirements, while also engaging continuously and employing an appropriate array of non-judicial subject-matter experts. A number of other issues were also raised, in terms of ensuring independence in practice, incorporating points of friction, and separating the authorization and ongoing supervision phases. In terms of

113. One example includes the ability of the U.K.'s Equality and Human Rights Commission to bring or intervene in judicial review proceedings. *See R (On the application of Privacy International) v. Investigatory Powers Tribunal and others* [2019] UKSC 22.

the authorization phase, highlighted issues include the importance of authorization at both the collection and access to data stages, the margin of appreciation that may be permitted to the security services or the executive, and the scope of review. In terms of the ongoing supervision phase, issues of interest include the resources necessary to ensure effective oversight, including technical expertise, and the need for longer term thematic review, as well as the importance of links between the oversight mechanism and the ex post facto review tribunal.