JUDICIAL OVERSIGHT OF INTERCEPTION OF COMMUNICATIONS IN THE UNITED KINGDOM: AN HISTORICAL AND COMPARATIVE ANALYSIS

David G. Barnum*

TABLE OF CONTENTS

I. INTRODUCTION ............................................................................... 239

II. CONSTRUCTING AN INTERCEPTION REGIME IN THE UNITED KINGDOM: THE ANGLO-AMERICAN AND EUROPEAN CONTEXT ....245
   A. The Fourth Amendment and Wiretapping in the United States ........................................................................................ 246
      1. Katz v. United States ......................................................... 246
      2. Title III (1968) ................................................................... 246
      3. United States v. U.S. District Court (Keith) ...................... 248
      4. Foreign Intelligence Surveillance Act of 1978 .................. 249
      5. Conclusion ......................................................................... 252
   B. The European Convention and Wiretapping: Klass v. Germany ................................................................................... 253
      1. National Security and the Interception Power in Germany .......................................................................................... 253
      2. The Road to Strasbourg: Intervening Developments .......... 255
      3. Klass v. Germany ............................................................... 257
      4. Conclusion ......................................................................... 258

* Professor of Political Science, DePaul University. Ph.D., Stanford University, 1974; M.Sc., London School of Economics, 1966; B.A., Stanford University, 1964. I am indebted to Maurice Sunkin of the University of Essex and David Feldman of the University of Cambridge for helpful feedback on earlier versions of this Article. Any remaining errors are mine and mine alone.
III. INTERCEPTION OF COMMUNICATIONS IN THE UNITED KINGDOM .... 259
   A. Initial Developments, 1979–1985 ........................................ 259
      1. The Birkett Report (1957) ............................................. 260
      2. Malone v. Commissioner of Police of the Metropolis ...... 263
      3. The Decision in Malone .............................................. 264
      4. The Aftermath of Malone ............................................. 267
      5. The European Court of Human Rights Decision .......... 268
      6. Interception of Communications Act 1985 ................. 270
      7. The Interception of Communications Act and Individual Rights ........................................ 275
   B. The Run-up to RIPA, 1985–2000 ...................................... 276
      3. The Labour Government and Policy Change .......... 280
      4. The RIPA Debate in Parliament ..................................... 281
      6. Conclusion .................................................................. 284

IV. RIPA 2000 IN THE EUROPEAN COURT: THE KENNEDY CASE ......... 285
   A. The Article 8 Complaint ................................................... 286
   B. The Article 6 Complaint ................................................... 287
   C. Conclusion .................................................................. 290

V. COMPARING BRITISH AND AMERICAN SURVEILLANCE LAW ....... 291
   A. Structures, Procedures, and Operational Realities .......... 291
      1. Operational Realities of the Warrant-Granting Process ........................................ 293
      2. Ex Post Scrutiny of Authorized Wiretapping ............... 294
      3. Conclusion .................................................................. 296
   B. The Incidence of Wiretapping ......................................... 297
      1. Wiretapping in the United States ......................... 297
      2. Wiretapping in the United Kingdom ...................... 298
      3. Wiretapping in Other Jurisdictions ....................... 299
         a. Bulgaria ............................................................. 299
         b. Moldova ............................................................. 300
      4. Conclusion .................................................................. 301

VI. CONCLUSION ...................................................................... 301
I. INTRODUCTION

In the wake of Edward Snowden’s revelations about the systematic acquisition by the National Security Agency (NSA) of telephone metadata and internet information—and about cooperation between the NSA and its counterpart in the United Kingdom, the Government Communications Headquarters (GCHQ), in such acquisition—the British Foreign Secretary, William Hague, addressed the House of Commons.1 As Foreign Secretary, Hague was responsible for issuing warrants to GCHQ for interception of international and wholly foreign communications. In his prepared remarks, Hague said that:

At [the heart of the strong framework of democratic accountability and oversight that governs the use of secret intelligence in the United Kingdom] are two Acts of Parliament: the Intelligence Services Act 1994 and the Regulation of Investigatory Powers Act 2000.2 The Acts require GCHQ and other agencies to seek authorisation for their operations from a Secretary of State, normally the Foreign Secretary or Home Secretary. . . . This combination of needing a warrant from one of the most senior members of the Government, decided on the basis of detailed legal advice, and such decisions being reviewed by independent commissioners and implemented by agencies with strong legal and ethical frameworks, with the addition of parliamentary scrutiny by the [Intelligence and Security Committee]3 . . . provides one of the strongest systems of checks and balances and democratic accountability for secret intelligence anywhere in the world.4

In the discussion that followed, the Foreign Secretary took questions from members of Parliament. Among the questioners was Labour MP Jack Straw,

the Secretary of State [would] accept that many of our allies, leaving aside the United States, are astonished by the degree of control and supervision of our system of ministerial oversight, oversight by judicially qualified commissioners and oversight by the [Intelligence and Security Committee], which surpasses that of most other western democracies?  

Hague responded that “[t]he right honorable Gentleman is absolutely right. . . . [A]s he knows very well, the system of checks and balances and scrutiny that we have is among the strongest in the world; it could be the strongest in the world.”

In the United States, Snowden’s revelations were followed by, among other things, a series of press releases by the Director of National Intelligence, James Clapper. In a statement released on June 6, 2013, Clapper said that “[t]here is a robust legal regime in place governing all activities conducted pursuant to the Foreign Intelligence Surveillance Act, which ensures that those activities comply with the Constitution and laws and appropriately protect privacy and civil liberties.” In a similar vein, in a blog post on June 11, 2013, security expert and former NSA Inspector General Joel Brenner wrote that:

The United States has the most expensive, elaborate, and multi-tiered intelligence oversight apparatus of any nation on Earth. We have well staffed intelligence committees in the House and Senate. The National Security Division of the Justice Department rides herd on the intelligence agencies. The FISA Court gets detailed reports of collection under its orders. The NSA has a robust compliance organization. It also has an inspector general with wide powers operating outside the chain

---

5 Id. at col. 38.
6 Id.
of command. None of our European allies controls intelligence activities with comparable rigor.8

It is understandable that officials and experts in both Britain and the United States would be anxious to stress the superiority of their respective systems of authorization and oversight of interception of communications. Presumably they cannot all be right, but this does not preclude the possibility that policy makers in both countries have established satisfactory mechanisms for overseeing the surveillance activities of executive branch officials, and have thereby arguably, if approximately, realized the proverbial goal of striking a “proper balance” between liberty and security.

This Article will examine the origin and development of modern arrangements for authorization and oversight of interception of communications within the United Kingdom. It will then venture some comparative conclusions. In particular, it will examine the role of the European Court of Human Rights (ECtHR) in shaping the contours of British surveillance law and in passing judgment on the “Convention-compatibility,” pursuant to the court’s power to enforce the human rights provisions of the European Convention on Human Rights (ECHR), of the surveillance regime that Britain eventually adopted.9 In addition, the Article will compare the surveillance regimes of Britain and the United States with reference to both their statutory underpinnings and available statistical information about their practical operation.

---


It is important at the outset to emphasize the limited scope of the ensuing discussion. The phrase “interception of communications” has many meanings. In particular, questions of the legality of government access to the content of communications—the core of the present analysis—bleed inexorably into questions regarding the legal status of non-content “communications data,” such as phone numbers and email addresses, and of various categories of “stored communications.” In addition, both governments and private-sector organizations are steadily perfecting their ability to engage in “data mining” of the vast amounts of heretofore largely inaccessible information that is now available in digital form. Finally, trends in surveillance practices cannot easily be separated from overarching concerns about the demise of privacy in modern society and the role of technology in transforming the relationship between citizens, private-sector institutions, and the state.\(^{10}\)

The discussion that follows will not attempt to explore more than a small corner of the overall problem of government surveillance and privacy rights. Analysis will be confined to examining the real-time acquisition of the content of telephone conversations, that is, “traditional wiretapping,” or what today might even be called “old-fashioned wiretapping.” In addition, the Article will focus primarily, although not exclusively, on the history and modern content of the law of telephone wiretapping in Britain and the United States.\(^{11}\)


Finally, the Article will be confined to examining “domestic” or “internal” surveillance, as distinct from “strategic” or “external” surveillance (often described as the collection of “signals intelligence”). “Domestic” or “internal” surveillance is usually understood to encompass the use within national boundaries of electronic devices and/or covert human operatives to target individuals who are themselves located within the national boundary. “Strategic” or “external” surveillance, on the other hand, usually refers to the use of surveillance capabilities to monitor international or wholly external communications. The distinction between the two forms of surveillance is almost certainly becoming less tenable with every passing day. However, legislative enactments and court decisions in both the United States and Europe have for many years distinguished between surveillance that consists of tracking individuals through deployment of domestic surveillance capabilities—even if the individuals are non-citizens or the threats they pose originate in foreign countries—and surveillance strategies aimed at systematically monitoring international or wholly external communications or targeting persons located outside of national boundaries.\(^\text{12}\) The discussion

---


More recently, in response to claims by ten human rights organizations—including Liberty, Privacy International, and Amnesty International—the UK’s Investigatory Powers Tribunal (IPT) issued a series of public rulings. The claimants alleged that the surveillance activities of GCHQ, including its bulk collection of both the content and metadata of telephone and internet communications, and its collaboration with the NSA in such collection, were incompatible with Article 8 of the ECHR and illegal under the UK’s regulation of Investigatory Powers Act 2000 (RIPA 2000). In two initial rulings, the IPT rejected most of the claimants’ allegations, including the core allegation that GCHQ’s bulk collection activities were incompatible with Article 8 and illegal under RIPA 2000. See Liberty v. GCHQ, [2014] UKIPTrib13/77-H, available at http://www.ipt-uk.com/docs/IPT_13_168-173_H.pdf; Liberty v. Secretary of State for Foreign and Commonwealth Affairs, [2015] UKIPTrib 13/77-H, available at http://www.ipt-uk.com/docs/Liberty_Ors_Judgment_6Feb15.pdf. In a third ruling, the IPT held that interception of emails of two of the ten NGOs—the Egyptian Initiative for Personal Rights (EIPR) and the South African-based Legal Resources Centre (LRC)—had been lawful under RIPA but had breached Article 8 because of GCHQ’s failure to follow its own procedures governing the length of time during which emails were retained.
that follows will be confined, insofar as it is possible to do so, to the former.\footnote{Edward Snowden’s revelations have primarily focused on the conduct of external surveillance and the bulk collection of telephone and internet metadata by the NSA, GCHQ, and other intelligence agencies. The ensuing analysis will therefore not address them in any detail.}

The remainder of this Article will be divided into four parts. Part II will briefly explore the transnational legal environment with which British policy makers were confronted when they reexamined their interception practices in the late 1970s. Most prominent in this respect were various court decisions and legislative enactments of which the surveillance regimes of the United States and Germany were comprised.


Part IV will examine the ECtHR’s decision in \textit{Kennedy v. United Kingdom} (2010). The case served as a vehicle for the court’s decision and the way in which particular emails were selected for further examination. The tribunal informed the other eight claimants in the litigation that “no determination had been made in [their] favour,” leaving them in doubt about whether their communications had been intercepted in the first place. See \textit{Liberty v. GCHQ}, [2015] UKIPTrib 13/77-H-2, available at https://s3.amazonaws.com/s3.documentcloud.org/documents/2108743/final-liberty-ors-open-determination.pdf. \textit{See also infra} notes 180–82 and accompanying text. On July 1, 2015, in an exceedingly embarrassing development, the tribunal sent an email to Amnesty International admitting that it was Amnesty rather than the Egyptian organization whose emails had been lawfully collected but mishandled by GCHQ after their initial collection. This, of course, constituted official proof that GCHQ had been systematically collecting Amnesty’s emails and conceivably examining and making further use of some of them. See Owen Bowcott, \textit{GCHQ spied on Amnesty International, tribunal tells group in email}, \textit{The Guardian} (July 1, 2015), available at http://www.theguardian.com/uk-news/2015/jul/01/gchq-spied-amnesty-international-tribunal-email. In the meantime, on April 10, 2015, all ten organizations submitted an application to the ECtHR challenging the IPT’s initial rulings upholding the legality and Convention-compatibility of GCHQ’s bulk collection activities. See \textit{The European Court of Human Rights Application: 10 Human Rights Organisations v United Kingdom, Additional Submissions on the Facts and Complaints}, AMNESTY INT’L (Apr. 9, 2015), https://www.amnesty.org/en/documents/ior60/1415/2015/en/.

Finally, Part V will compare the British and American approaches to authorization and oversight of interception of communications. By now, the British system of executive warrants is well established, and has received the imprimatur of the ECtHR. It does not exist in a vacuum, however, but operates in conjunction with a set of quasi-judicial mechanisms for overseeing executive branch surveillance activities. In the United States, ordinary courts and the FISA Court continue to be solely responsible for pre-approving executive branch surveillance and for reviewing the lawfulness of such surveillance when it is challenged. Which system does a better job of enabling government to combat crime and protect national security, while simultaneously constraining abuses of executive power and safeguarding citizens’ rights, remains a surprisingly open question.

II. CONSTRUCTING AN INTERCEPTION REGIME IN THE UNITED KINGDOM: THE ANGLO-AMERICAN AND EUROPEAN CONTEXT

The British were forced by circumstances to reexamine their approach to interception of communications in the late 1970s. At that time, awareness of foreign judicial precedent was growing among human rights activists in many jurisdictions, including Britain. In addition, the decision-making institutions of the Council of Europe, including the ECtHR, were becoming more assertive. The upshot was that British judges and other policy makers were obliged to respond to transnational developments in surveillance law and privacy rights that in earlier decades might have been dismissed as irrelevant. The two most prominent bodies of non-British law were the constitutional rulings of the U.S. Supreme Court and the emerging jurisprudence of the ECtHR.

14 See infra Part III.
A. The Fourth Amendment and Wiretapping in the United States

1. Katz v. United States

In 1967, in *Katz v. United States*, the U.S. Supreme Court held that wiretapping and third party bugging by law enforcement officials requires a judicial warrant based on probable cause. *Katz* brought to a close a period of nearly forty years during which wiretapping had not been subject to Fourth Amendment restraint. In the Court’s initial encounter with wiretapping, *Olmstead v. United States*, Chief Justice Taft, writing for a five-to-four majority, noted that “[t]here was no entry of the houses or offices of the defendants,” nor any seizure of “tangible material effects.” As a result, he concluded, “the wire tapping here disclosed did not amount to a search or seizure within the meaning of the Fourth Amendment.” Some four decades later—in *Katz*, a case involving a variation on the technique of third party bugging—the Court concluded that the government’s activities “violated the privacy upon which [the petitioner] justifiably relied . . . and thus constituted a ‘search and seizure’ within the meaning of the Fourth Amendment.” The Court then held that “the usual requirement of advance authorization by a magistrate upon a showing of probable cause” would henceforth be “a constitutional precondition of the kind of electronic surveillance involved in this case.”

2. Title III (1968)

Seven months after the *Katz* decision, Congress enacted the Omnibus Crime Control and Safe Streets Act of 1968, Title III of which remains the principal federal legislation regulating interception of communications in

---

16 277 U.S. 438 (1928).
17 Id. at 464.
18 Id. at 466.
19 Id.
20 Law enforcement agents had overheard one end of a telephone conversation by attaching a device to the outside of a public telephone booth. Id. at 348.
21 Id. at 353.
22 Id. at 358–59.
ordinary criminal cases. As amended by the Electronic Communications Privacy Act of 1986, Title III makes it a crime for “any person [to] intentionally intercept . . . any wire, oral, or electronic communication.” However, the Attorney General or other specially designated high-level Department of Justice officials “may authorize an application to a Federal judge of competent jurisdiction for . . . an order authorizing or approving the interception of wire or oral communications by the Federal Bureau of Investigation [or other federal agency] when such interception may provide [evidence of the commission of various specified federal offenses].” The judge to whom an application is made is authorized to enter an ex parte order approving interception if he or she determines that “there is probable cause for belief that an individual is committing, has committed, or is about to commit a [specified] offense.”

Title III contains a mandatory—and rather generous—post-surveillance notification provision. Under section 2518(8)(d),

> within a reasonable time but not later than ninety days . . . the issuing or denying judge shall cause to be served, on the persons named in the order or the application, and such other parties to intercepted communications as the judge may determine in his discretion that is in the interest of justice, an inventory which shall include notice of . . . the fact of the entry of the order or the application [and the fact that] communications were or were not intercepted.

The judge may also “in his discretion make available to such person or his counsel for inspection such portions of the intercepted communications, applications and orders as the judge determines to be in the interest of justice.”

---

25 Id. § 2516(1).
26 Id. § 2518(3)(a).
28 Id. § 2518(8)(d). For further discussion of the post-surveillance notification requirements of the Foreign Intelligence Surveillance Act of 1978, see infra notes 48–54 and accompanying text. For discussion of the post-surveillance notification requirements of German and British interception law, see infra notes 61–80, 169–85, 252–70 and accompanying text.
Title III contains a statutory exclusionary rule and numerous other safeguards against executive branch abuse of the power to wiretap in criminal cases. The safeguards are so numerous, in fact, that congressional regulation of such surveillance has been described as imposing “a super-warrant requirement for telephones,” and the Department of Justice itself readily admits that “several of Title III’s provisions are more restrictive than what is required by the Fourth Amendment.”

The Supreme Court’s decision in *Katz* and Congress’s passage of Title III fundamentally revamped the law of electronic surveillance in the United States. In particular, they firmly established the necessity of judicial pre-approval of executive branch use of electronic surveillance in ordinary criminal investigations. What neither *Katz* nor Title III resolved, however, was the question of executive branch power to wiretap or engage in other forms of covert surveillance to protect against alleged threats to national security.

3. United States v. U.S. District Court (Keith)

The Supreme Court addressed the existence and scope of a national security exception to the Fourth Amendment’s warrant requirement in *United States v. U.S. District Court (Keith)*. *Keith* involved an alleged plot by domestic radicals to bomb a CIA office in Ann Arbor, Michigan. The Nixon Administration argued that the government was exempt from the need to obtain a judicial warrant whenever it believed it was dealing not with ordinary criminal activity but instead with a domestic threat to national security. Justice Powell, writing for the majority, diplomatically but firmly rejected the government’s position. He acknowledged the government’s concerns—that the collection of intelligence is different from the gathering of evidence, that courts would be ill-equipped to make probable cause determinations in national security cases, and that the need to request judicial approval would jeopardize the secrecy of intelligence-gathering.
operations—but concluded that such concerns “do not justify departure in this case from the customary Fourth Amendment requirement of judicial approval prior to initiation of a search or surveillance.”

Justice Powell ended his opinion by noting that the Court’s decision was confined to “the domestic aspects of national security” and did not purport to address “the issues which may be involved with respect to activities of foreign powers or their agents.” He also noted that even though the Court was holding “that prior judicial approval is required for the type of domestic security surveillance involved in this case,” Congress might decide that “the application and affidavit showing probable cause [in domestic security cases] need not follow the exact requirements of [Title III]” and also that “the request for prior court authorization could, in sensitive cases, be made to any member of a specially designated court.”

Justice Powell thus extended an invitation to Congress to implement the reasonableness requirement of the Fourth Amendment in domestic security cases by enacting legislation that required prior judicial approval of electronic surveillance but exempted executive officials from the rigorous demands of Title III. Congress did not immediately respond. When it did, however, it produced legislation that closely tracked Powell’s suggestions. What Congress also did, however, was to implement those suggestions in legislation aimed at regulating executive branch use of electronic surveillance in foreign security cases—that is, addressing the constitutional issue upon which the Court had expressly refrained from passing judgment.

4. Foreign Intelligence Surveillance Act of 1978

In the Foreign Intelligence Surveillance Act of 1978 (FISA), Congress created a seven-judge special court, known as the “FISA Court” or the “FISC,” which was given jurisdiction to “hear applications for and grant orders approving electronic surveillance anywhere within the United States under the procedures [established by FISA].” Orders may be sought from

---

36 Id.
37 Id. at 321.
38 Id. at 321–22.
39 Id. at 324.
40 Id. at 323.
42 50 U.S.C. § 1803(a)(1). The FISA Court was subsequently enlarged from seven to eleven judges by section 208 of the USA PATRIOT Act. See Uniting and Strengthening
the court when the target of proposed surveillance is either a “foreign power” or “an agent of a foreign power,” and “a significant purpose of the surveillance is to obtain foreign intelligence information.” The judge to whom an application is made is authorized to issue an order if he or she finds that “there is probable cause to believe that [the] target of the electronic surveillance is a foreign power or an agent of a foreign power.”

Applications to the FISA Court ordinarily originate with the FBI, but are reviewed by Department of Justice lawyers before presentation to the Attorney General for his or her approval. Since 2006, responsibility for preparing and filing applications for FISA Court orders has been assigned to the National Security Division of the Justice Department.

In contrast to Title III, FISA contains nothing resembling a “mandatory” or “generous” mechanism for post-surveillance notification of targeted persons. Under FISA, the target of electronic surveillance does not become an “aggrieved person” entitled to notification unless the government intends to enter into evidence any information obtained or derived from the surveillance “in any trial, hearing, or other proceeding.” In addition, whenever an aggrieved person files a motion “to discover or obtain applications or orders or other materials relating to electronic surveillance”—as a prelude, presumably, to filing a motion to suppress FISA-derived evidence—the Attorney General is authorized to file an affidavit under oath

44 Id. § 1804(a)(6)(B).
48 50 U.S.C. § 1806(c). Under the statute, an “aggrieved person” is defined as “a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance.” Id. § 1801(k).
with the court “that disclosure or an adversary hearing would harm the national security of the United States.”\footnote{Patricia L. Bellia, Designing Surveillance Law, 43 Ariz. St. L.J. 293, 341 (2011) (noting that “more that 28,000 FISA applications and renewals [have been] granted since 1979,” that “challenges to introduction of FISA-derived evidence or demands for disclosure of [such] evidence have been raised in approximately thirty-five cases,” and that “none of these challenges has been successful”).} The court is instructed to respond by “review[ing] \textit{in camera} and \textit{ex parte} the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted.”\footnote{United States v. Daoud, No. 12CR723, 2014 U.S. Dist. LEXIS 10716 (N.D. Ill. Jan. 29, 2014).} In making this determination, the court is authorized to disclose to the aggrieved person “portions” of the relevant materials, but “only where such disclosure is necessary to make an accurate determination of the legality of the surveillance.”\footnote{United States v. Daoud, 755 F.3d 479 (7th Cir.), \textit{supplemented}, 761 F.3d 678 (7th Cir. 2014), \textit{cert. denied}, 135 S. Ct. 1456 (2015). The Seventh Circuit concluded that the district judge failed to fulfill “her obligation to evaluate the parties’ allegations in light of the FISA materials to determine whether she could assess the legality of those materials herself, without disclosure of them to [the defendant’s] lawyers.” 755 F.3d at 483. The court then held that disclosure of the classified materials was not necessary and that the government’s investigation “did not violate FISA.” \textit{Id.} at 485. On July 14, 2014, the Seventh Circuit issued a heavily redacted classified opinion explaining its conclusions, \textit{see id.} 761 F.3d 678, and on February 23, 2015, the Supreme Court, without opinion, denied the defendant’s petition for a writ of certiorari. \textit{See id.} 135 S. Ct. 1456.}

Since FISA’s passage in 1979, it has been exceedingly rare for FISA-based surveillance to culminate in a criminal prosecution or other judicial proceeding. As a result, persons targeted for such surveillance are unlikely to be aware of that fact. In addition, given the phrasing of section 1806(f), criminal defendants who do seek disclosure of FISA-derived evidence are unlikely to succeed. Prior to 2014, no judge had ever ordered the government to disclose to a defendant the materials on which the FISA Court’s warrant or warrants had been based.\footnote{United States v. Daoud, No. 12CR723, 2014 U.S. Dist. LEXIS 10716 (N.D. Ill. Jan. 29, 2014).} In 2014, a district judge ordered disclosure for the first time,\footnote{United States v. Daoud, 755 F.3d 479 (7th Cir.), \textit{supplemented}, 761 F.3d 678 (7th Cir. 2014), \textit{cert. denied}, 135 S. Ct. 1456 (2015). The Seventh Circuit concluded that the district judge failed to fulfill “her obligation to evaluate the parties’ allegations in light of the FISA materials to determine whether she could assess the legality of those materials herself, without disclosure of them to [the defendant’s] lawyers.” 755 F.3d at 483. The court then held that disclosure of the classified materials was not necessary and that the government’s investigation “did not violate FISA.” \textit{Id.} at 485. On July 14, 2014, the Seventh Circuit issued a heavily redacted classified opinion explaining its conclusions, \textit{see id.} 761 F.3d 678, and on February 23, 2015, the Supreme Court, without opinion, denied the defendant’s petition for a writ of certiorari. \textit{See id.} 135 S. Ct. 1456.} but the decision was emphatically reversed by the Seventh Circuit Court of Appeals.\footnote{United States v. Daoud, 755 F.3d 479 (7th Cir.), \textit{supplemented}, 761 F.3d 678 (7th Cir. 2014), \textit{cert. denied}, 135 S. Ct. 1456 (2015). The Seventh Circuit concluded that the district judge failed to fulfill “her obligation to evaluate the parties’ allegations in light of the FISA materials to determine whether she could assess the legality of those materials herself, without disclosure of them to [the defendant’s] lawyers.” 755 F.3d at 483. The court then held that disclosure of the classified materials was not necessary and that the government’s investigation “did not violate FISA.” \textit{Id.} at 485. On July 14, 2014, the Seventh Circuit issued a heavily redacted classified opinion explaining its conclusions, \textit{see id.} 761 F.3d 678, and on February 23, 2015, the Supreme Court, without opinion, denied the defendant’s petition for a writ of certiorari. \textit{See id.} 135 S. Ct. 1456.}

Although the interception regime established by FISA does require prior judicial approval of wiretapping and other forms of electronic surveillance, it otherwise is not notably transparent. In the United States, targets of FISA
surveillance are not notified of that fact unless the government intends to initiate some form of judicial proceeding, and no defendant who has tried to gain access to FISA-derived evidence has ever succeeded in doing so. This fact should be kept in mind in evaluating the British approach to interception of communications, which strikes many observers as being exceptionally secretive. Putting to one side the relative merits of a dispersed system of judicial warrants versus a centralized system of executive warrants, it is clear that overwhelming secrecy surrounds both the British and the American approaches to authorization and oversight of domestic surveillance of targets perceived to constitute a national security threat.55

5. Conclusion

By 1978, the necessity of judicial oversight of the executive branch’s use of electronic surveillance was firmly established in American law. In the late 1960s, both Katz and Title III made plain that wiretapping in ordinary criminal cases was subject to judicial oversight. In 1972, Keith extended the Fourth Amendment’s warrant requirement to executive branch wiretapping in cases involving an alleged domestic threat to national security, holding that such surveillance “requires an appropriate prior warrant procedure.”56 Six years later, in FISA, Congress translated the Supreme Court’s insistence on “an appropriate prior warrant procedure” into legislation that addressed foreign threats to national security within the United States by requiring the government to obtain judicial pre-approval for wiretapping of any person suspected of being “an agent of a foreign power.”57 In so doing, Congress put in place the final components of a national policy in which internal or domestic use of wiretapping and other forms of electronic surveillance, in both criminal investigations and intelligence-gathering operations, is governed by the Fourth Amendment, and the commencement of surveillance by executive branch officials in individual cases is contingent upon the acquisition of a judicial warrant.

55 The secrecy surrounding the warrant-granting process in the United Kingdom is discussed in infra notes 114, 169–85, 252–70 and accompanying text.
56 United States v. U.S. District Court (Keith), 407 U.S. at 320.
B. The European Convention and Wiretapping: Klass v. Germany

Presumably by sheer coincidence, the year in which the U.S. Congress passed FISA was also the year in which the issue of executive branch wiretapping became the focus, for the first time, of European-level human rights scrutiny. The vehicle, Klass v. Germany, involved a challenge to German surveillance legislation alleged to violate Article 8 of the ECHR, and it resulted in the ECtHR’s first-ever decision on the interplay between internal surveillance regimes and fundamental human rights law.58

1. National Security and the Interception Power in Germany

In 1968, the German Parliament enacted national legislation to govern the use of telephone wiretapping by both the police in criminal investigations and intelligence-gathering officials in national security investigations.59 The legislation, known as the “G10 statute,” established a bifurcated system. Whereas wiretapping by the police required judicial pre-approval, wiretapping by intelligence-gathering officials was governed by separate provisions designed to enable the government to respond to perceived threats with greater speed and secrecy.60

60 Article II of the statute dealt with wiretapping for law enforcement purposes and is incorporated as sections 100a-101 of the German Code of Criminal Procedure Code (Strafprozessordnung). See Carr, supra note 59, at 607 n.2; Paul M. Schwartz, German and U.S. Telecommunications Privacy Law: Legal Regulation of Domestic Law Enforcement Surveillance, 54 HASTINGS L.J. 751, 791–94 (2003). Article I of the statute authorized the use of wiretapping for intelligence and national security purposes. The common reference to the law as the “G10 statute”—or simply as the “G10”—was based on the fact that passage of the law was immediately preceded by the passage by Parliament of amendments to Article 10 of the Constitution of the Federal Republic (the Grundgesetz or “Basic Law”). The dual purpose of the amendments was to exempt the government from the need to get a judicial warrant in national security cases and to confer prospective constitutional legitimacy on the G10. Klass, App. No. 58243/00, 28 Eur. Ct. H.R. paras. 15-25.
The G10 authorized procedures for wiretapping in national security cases that differed in two principal ways from the rules that governed police wiretapping. First, whereas post-surveillance notification was the norm in criminal cases, the statute prohibited notifying anyone who had been targeted for national security surveillance. The statute created a mechanism for intelligence-gathering officials to initiate surveillance without receiving a judge’s pre-approval. At the federal level, the statute provided that requests for permission to wiretap could originate with various agencies responsible for counterintelligence and military defense. Two executive officials, the Minister of the Interior (in the case of domestic or internal surveillance) and the Minister of Defense (in the case of strategic or external surveillance), were authorized to issue warrants and were required to do so personally.

Two bodies were responsible for overseeing the ministers’ decisions to issue warrants. The first was a five-person board consisting of members of Parliament representing a cross-section of political parties, including the opposition, which was responsible for reviewing a semi-annual report prepared by each of the ministers (G10 Board). An additional and more important responsibility of the G10 Board was to appoint a three-person “G10 Commission.” Under the law as written, each minister was “bound every month to provide . . . an account [to the Commission] of the measures he has ordered.” In addition, the Commission was authorized to review wiretap orders and to entertain applications from persons who believed themselves to be under surveillance. The Commission could require immediate termination of any interception order which it deemed “illegal or unnecessary.”

The G10 statute was challenged by a group of public officials and lawyers who alleged that it violated Article 8 of the European Convention. Article 8 consists of two paragraphs. The first paragraph guarantees that “[e]veryone has the right to respect for his private and family life, his home

62 Id. para. 18.
65 Id. para. 21. The chairman of the G10 Commission was required to be someone “qualified to hold judicial office.” Id.
66 Id. para. 21.
67 Id. para. 10.
and his correspondence.” The second paragraph qualifies this right by stipulating that “[t]here shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests [inter alia] of national security . . . [or] for the prevention of disorder or crime . . . .”

The plaintiffs in *Klass* argued that the G10 statute violated Article 8 for two reasons: first, they objected to the fact that in national security cases, the G10 eliminated judicial pre-approval of wiretapping and substituted a system of executive or ministerial warrants. Second, they contended that the law violated Article 8 because it permitted the government to conduct covert surveillance of persons deemed to constitute a threat to national security “without obliging the authorities in every case to notify the persons concerned after the event.”

### 2. The Road to Strasbourg: Intervening Developments

The *Klass* case reached the ECtHR in 1978. Prior to reaching the court, however, two important developments occurred. First, the German Federal Constitutional Court examined the validity of the G10 statute under the German Constitution and reached two main conclusions. First, the German court upheld the constitutional validity of executive or ministerial warrants in conjunction with ex post review of the lawfulness of ministers’ decisions by the G10 Commission. The court concluded that the Commission “provid[ed] as effective [control] of the surveillance as the judiciary provided for wiretaps sought under the authority of the criminal law.”

---

68 ECHR, *supra* note 9, art. 8(1).
69 Id. art. 8(2).
71 Id. The plaintiffs in *Klass* were not required to allege that they had in fact been wiretapped because, by American standards, standing requirements in Article 8 cases involving covert surveillance are effectively eliminated. The ECtHR decided the standing issue by “accept[ing] that an individual may, under certain conditions, claim to be the victim of a violation [of his or her Article 8 rights] occasioned by the mere existence . . . of legislation permitting secret measures, without having to allege that such measures were in fact applied to him.” *Id.* para. 34 (emphasis in original).
73 The court concluded that the Commission “provid[ed] as effective [control] of the surveillance as the judiciary provided for wiretaps sought under the authority of the criminal law.” Schwartz, *supra* note 60, at 775 (citing 30 BVerfGE, 1 (23) (Ger.)).
concluded that section 5(5) of the law, which mandated a blanket ban on post-surveillance notification of targeted persons, was incompatible with the German Constitution because it prohibited "informing the affected party about the restrictive measures [even] when it can occur without endangering the goal of the restriction."74

The second development that antedated the ECtHR's decision in Klass was a substantial expansion of the de facto role of the G10 Commission. In the G10 statute as written, the Commission was confined to conducting a once-a-month ex post review of ministers’ wiretap orders.75 After 1970, however, "apparently responsive to political considerations, [federal Interior Ministers adopted] a policy of presenting applications [for surveillance orders] to the G-10 Commission for prior review and approval."76

The G10 statute as written also prescribed that none of the targets of national security surveillance was entitled to post-surveillance notification.77 The German Constitutional Court in its 1970 "Monitoring Opinion" had decided that post-surveillance notification was sometimes required, but it had not delineated "when notice would be required, or who (i.e., the G-10 Commission or the Interior Minister) was to decide whether notice was to be provided."78 In the wake of the Federal Constitutional Court’s decision, however, ministers began the practice of submitting to the G10 Commission their decisions to withhold notification, and the Commission assumed de facto power to "direct the Minister to inform the person concerned that he has been subjected to surveillance measures."79 Therefore by 1978, the ECtHR was not only conscious of the greatly expanded role of the G10 Commission, but was also aware that the German government intended to formalize the Commission’s role in proposed amendments to the G10 statute.80

In sum, between 1968 and 1978 two main events occurred. First, the Federal Constitutional Court issued its 1970 decision requiring post-surveillance notification of some but not all targets of national security

74 Id. at 776 (quoting BVerfGE, 30 (32) (Ger.)). See also Klass, App. No. 58243/00, 28 Eur. Ct. H.R. para. 11.
76 Carr, supra note 59, at 622.
78 Carr, supra note 59, at 613.
80 Id. para. 21. The amendments were enacted on September 13, 1978, one week after the Klass decision was handed down. Carr, supra note 59, at 613 n.50.
surveillance. Second, the G10 Commission assumed de facto power both to pre-approve ministers’ decisions to initiate surveillance and to withhold post-surveillance notification. These developments presumably made the ECtHR’s task of deciding whether the G10 statute was compatible with Article 8 of the ECHR considerably easier than it might otherwise have been.

3. Klass v. Germany

The ECtHR began its assessment by asserting—in a passage that is reiterated without fail in all of its post-Klass surveillance decisions—that the court “must be satisfied that, whatever system of surveillance is adopted, there exist adequate and effective guarantees against abuse.” It then noted that in the area of executive branch electronic surveillance, “it is in principle desirable to entrust supervisory control to a judge.” However, the court concluded that the G10 Board and the G10 Commission “are independent of the authorities carrying out the surveillance, and are vested with sufficient powers and competence to exercise an effective and continuous control.” It followed, in the court’s view, that “the exclusion of judicial control does not exceed the limits of what may be deemed necessary in a democratic society.”

On the post-surveillance notification issue, the ECtHR expressed skepticism that it was “feasible in practice to require subsequent notification in all cases.” It chose instead to endorse the compromise adopted by the Federal Constitutional Court, that is, to require post-surveillance notification “as soon as notification can be made without jeopardising the purpose of the restriction.” The ECtHR then reached its final conclusion that “the German legislature was justified to consider the interference resulting from [the G10 statute] with the exercise of the right guaranteed by Article 8(1) as being necessary in a democratic society in the interests of national security and for the prevention of disorder or crime (Art. 8(2)).”

81 See supra notes 74, 77–79 and accompanying text.
82 Klass, App. No. 58243/00, 28 Eur. Ct. H.R. paras. 19, 21
83 Id. para. 50.
84 Id. para. 56.
85 Id.
86 Id.
87 Id. para. 58.
88 Id.
89 Id. para. 60.
4. Conclusion

*Klass* achieved a variety of objectives. First, the decision signaled that written legislation authorizing and regulating the exercise of interception of communications by executive branch officials was desirable, and perhaps even imperative. Second, it adopted a generous approach to standing, whereby an individual could challenge existing surveillance legislation “without having to allege that such measures were in fact applied to him.”90 Third, it held that in the context of intelligence gathering and the protection of national security, mechanisms for overseeing executive branch electronic surveillance other than pre-approval by courts were permissible, provided they incorporated “adequate and effective guarantees against abuse.”91

Finally, *Klass* suggested that in national security cases, a blanket prohibition on notification of targeted persons would violate the ECHR. However, by the time the case reached the ECtHR, the G10’s blanket prohibition had been preemptively excised from the law by the Federal Constitutional Court, which required selective post-surveillance notification as a matter of domestic German constitutional law.92 Thus, it cannot be said that *Klass* precluded the possibility that a blanket ban on post-surveillance notification in national security cases would be consistent with the ECHR.

In addition, *Klass* necessarily failed to address the role of Article 8 in placing constraints on the power of government to engage in interception of communications in ordinary criminal cases. In particular, the decision left open two questions. The first was whether a system that excluded courts from playing any role in pre-approving law enforcement officials’ interception decisions would violate the ECHR. The second was whether, in ordinary criminal cases, the ECHR would permit a selective ban, let alone a blanket ban, on post-surveillance notification of targeted persons. A brewing challenge to British arrangements for interception of communications by executive branch officials in both national security investigations and ordinary criminal cases provided a vehicle for the ECtHR to scrutinize these important issues.

90 *Id.* para. 34; *see also supra* note 71 and accompanying text.
92 *See supra* note 74 and accompanying text.
III. INTERCEPTION OF COMMUNICATIONS IN THE UNITED KINGDOM

The interplay of judicial and legislative decisions that led eventually to the ECtHR’s 2010 opinion in Kennedy v. United Kingdom took three full decades to unfold. From 1979–1985, an initial round of developments occurred that focused on the issue of telephone tapping in criminal cases. This culminated in the passage of the Interception of Communications Act 1985. In the ensuing fifteen years, British policy makers struggled to respond to the ECtHR’s insistence on greater statutory regulation of the security services and of forms of covert surveillance other than wiretapping. In 2000, Parliament brought some closure to the events of this period by enacting the Regulation of Investigatory Powers Act.

A. Initial Developments, 1979–1985

The Klass decision was handed down on September 6, 1978. Only a few weeks earlier, an antiques dealer named James Malone had been on trial in London for the offense of handling stolen property. During the trial, it was revealed that Malone’s telephone had been tapped and that the police had intercepted at least one conversation. The trial ended partially in acquittal and partially in a mistrial, whereupon Malone instituted civil proceedings against the Metropolitan Police Commissioner in the Chancery Division of the High Court. The relief he sought was a declaration that the Police Commissioner had acted unlawfully by tapping Malone’s telephone, even though all parties to the litigation conceded that the tapping had been done pursuant to a warrant issued by the Home Secretary. Malone’s civil suit culminated, within Britain, with the issuance of a judgment by Vice-Chancellor Robert Megarry, Chief Judge of the Chancery Division of the High Court.

The Malone litigation brought to light a substantial array of obscure details about the practice of wiretapping in Britain. The information had been published in a 1957 report of the Committee of Privy Councillors

---

93 Simon Chesterman, “Ordinary Citizens” or A License to Kill? The Turn to Law in Regulating Britain’s Intelligence Services, 29 BUFF. PUB. INT. L.J. 1, 2 (2011).
94 Id.
95 Malone v. Comm’r of Police of the Metropolis (No. 2), [1979] 2 All E.R. 620 (Ch.).
96 Id.
97 For further discussion of the background of the Malone case and the decision of the High Court, see infra in notes 118–41 and accompanying text.
(Birkett Report). The Birkett Report may have been widely read at the time it was issued, but by the late 1970s its notoriety had faded. As a result, when its contents were disseminated anew in connection with the Malone decision, they came as a revelation to many.

1. The Birkett Report (1957)

The mandate of the Birkett Committee was to “report upon the exercise by the Secretary of State of the executive power to intercept communications.” In 1957, the post office was responsible for operating both the postal system and the telephone system. Thus, the Birkett Committee was charged with examining the role of the executive, in conjunction with the post office, in the interception of both postal and telephone communications.

With respect to the interception of postal communications, the Committee reported that statutes in force since 1710 forbid postal employees from opening mail except when authorized to do so “in obedience to an express warrant in writing under the hand of a Secretary of State.” With respect to telephone communications, the Committee discovered that the post office was likewise responsible for responding to government requests to engage in wiretapping—from both the police and the Security Service (MI5)—and that it had been doing so “from time to time since the introduction of the telephone.”

There was one important difference, however, between the power of the post office to open mail, on the one hand, and to tap telephones, on the other: the power to tap telephones had no statutory foundation. No provision of the Post Office Act 1953 or of any other parliamentary legislation expressly authorized the government to engage in telephone tapping, with or without a

---

98 COMMITTEE OF PRIVY COUNCILLORS, INQUIRY INTO THE INTERCEPTION OF COMMUNICATIONS, BIRKETT REPORT, 1957, Cmd. 283 (U.K.) [hereinafter BIRKETT REPORT], available at http://www.fipr.org/rip/Birkett.htm. The Committee was chaired by Lord Norman Birkett and thus bears his name.

99 Id. ¶ 1.
100 Id. ¶ 40.
101 Id. ¶ 39.
102 Id. ¶ 33 (quoting Post Office Act 1953, 1 & 2 Eliz. II, c. 36, §58(1) (U.K.), at the time the most recent version of the statute of 1710).
103 Id. ¶ 40.
104 Id. ¶ 27.
warrant issued by the Secretary of State. Consequently, the Committee reported that until 1937 “[n]o warrants by the Secretary of State were therefore issued.”

The Birkett Committee also learned, however, that in 1937 the government had decided that interception of telephone communications, like interception of postal communications, should be conditioned on a warrant issued by the Secretary of State for the Home Department. The decision extended the system of “executive” or “ministerial” warrants—that is, those issued by the Home Secretary, rather than a judge—to cover telephone tapping as well as the opening of mail. The extension was effected not by the passage of legislation, however, but by administrative fiat. Thus, the interception of telephone communications continued to lack any express statutory foundation.

The Birkett Committee then turned to the actual practice of wiretapping by government officials. It determined that the Home Secretary relied on established but unpublished criteria when deciding whether to issue a warrant. Three criteria governed the issuance of warrants to investigate ordinary criminal activity:

(a) The offence must be really serious.
(b) Normal methods of investigation must have been tried and failed [or] be unlikely to succeed if tried.
(c) There must be good reason to think that an interception would result in a conviction.

The Birkett Committee also examined the government’s use of telephone tapping to protect against threats to national security. The Committee determined that the Security Service (MI5) was responsible for wiretapping in such cases, and that it did so pursuant to a warrant issued by the Home Secretary. The Committee also learned that the criterion on which the

105 Id. ¶ 40.
106 Id.
107 Id. ¶ 41.
108 Id.
109 Id. ¶¶ 41–52.
110 Id. ¶ 64.
111 A “really serious” offense was defined as one that was punishable by three years’ imprisonment, or was an offense “of lesser gravity in which a large number of people were involved.” Id. ¶ 65.
112 Id. ¶ 64.
Secretary of State based decisions to issue a warrant was that “[t]here must be a major subversive or espionage activity that is likely to injure the national interest.”

A final important finding of the Birkett Committee concerned the use to which the evidence produced by a wiretap was put. The Committee reported that it was the unvarying practice of the Home Office not only to refrain from notifying persons who had been the targets of a wiretap, even in criminal cases, but also to scrupulously avoid using wiretap evidence in criminal prosecutions, and to respond to all inquiries by refusing to confirm or deny that telephone tapping had occurred at all.

The Birkett Committee then offered two broad conclusions. First, it noted that it has “been urged in some quarters that the authority for the issue of warrants for interception should not be left exclusively in the hands of the Secretary of State” and that the “chief suggested alternatives ... are that the Home Secretary should be assisted by an Advisory Committee or that warrants should be issued only on a sworn information before magistrates or a High Court judge.” The Committee responded that in its opinion,

neither of these proposals would improve matters. If a number of magistrates or judges had the power to issue such warrants, the control of the use to which methods of interception can be put would be weaker than under the present system. It might well prove easier in practice to obtain warrants.

The Committee’s second and overall conclusion was that it was satisfied that all the officers and officials concerned are scrupulous and conscientious in the use and exercise of the power to intercept communications. We are satisfied that interception is highly selective and that it is used only where

---

113 Id. ¶ 67.
114 Id. ¶ 152. The Home Office policy of never relying on wiretap evidence in individual cases has often been questioned but has never been abandoned. The most recent reaffirmation of the policy is the report of a cross-party group of Privy Counselors chaired by Sir John Chilcot. See Sec’y of State for the Home Dep’t, Intercept as Evidence, 2014, Cm. 8989 (U.K.), available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/388111/InterceptAsEvidence.pdf; see also infra notes 183–85 and accompanying text.
115 Birkett Report, supra note 98, ¶ 85.
116 Id. ¶ 86.
there is good reason to believe that a serious offence or security
interest is involved.117

2. Malone v. Commissioner of Police of the Metropolis

The 1957 Birkett Report continued to accurately describe the practice of
telephone tapping in Britain in 1979, when the High Court decided James
Malone’s civil suit against the Metropolitan Police Commissioner.118 The
litigation arose when, in the course of Malone’s 1978 criminal prosecution
for handling stolen property, a police sergeant inadvertently provided the
court with notes of a 1977 telephone conversation between Malone and
another.119 In doing so, of course, the sergeant had breached the long-
standing policy of the Home Office against courtroom disclosure of intercept
evidence.120 However, his misstep obliged the government to admit that in
accordance with policy—that is, on the authority of a warrant signed by the
Secretary of State—an interception had occurred.121 The trial ended
inconclusively, and while awaiting re-trial, Malone filed his suit in the High
Court.122

The lawsuit consisted of three main claims. First, Malone argued that
there was at common law a “right of privacy” that made it “unlawful for
anyone,” including the post office on the authority of a warrant issued by the
Secretary of State, “to intercept or monitor the telephone conversations of
another without the consent of that other.”123 Second, Malone argued that
telephone tapping as practiced in the United Kingdom violated Article 8 of
the ECHR “as construed by the European Court [in the Klass case].”124
Finally, Malone argued that telephone tapping as practiced in the United
Kingdom was unlawful because it was not based on “any grant of powers to
the executive to tap telephones, either by statute or by the common law.”125

117 Id. ¶ 123.
118 Malone, 2 All E. R. 620; see also supra notes 93–97 and accompanying text.
119 Malone, 2 All E. R. at 624.
120 See supra note 114 and accompanying text.
121 Malone, 2 All E. R. at 624.
122 Id. at 623–24.
123 Id. at 630.
124 Id.
125 Id.
3. The Decision in Malone

In the end, Vice-Chancellor Megarry dismissed all of Malone’s claims. In the course of a long and thoughtful judgment, however, he conscientiously addressed each of the plaintiff’s arguments. Malone’s first claim was that while the English common law might not recognize a general right of privacy, it did at least recognize “a particular right of privacy . . . to hold a telephone conversation in the privacy of one’s home without molestation.”126 To support this claim, Malone relied on the famous English general warrant cases, including *Entick v. Carrington*, and on the Fourth Amendment of the U.S. Constitution.

In *Entick v. Carrington*,127 Lord Camden had examined the legality of a search of Entick’s home for seditious literature under a general warrant issued by the Secretary of State, Lord Halifax.128 Camden concluded that in the absence of a clear common law or statutory basis for the exercise by the Secretary of State of the power to issue the warrant, the resulting search was an illegal trespass.129 Vice-Chancellor Megarry concluded, however, that Malone could not obtain “any assistance . . . from the general warrant cases.”130 Despite conceding that “there is admittedly no statute which in terms authorises the tapping of telephones, with or without a warrant,” Megarry found that

any conclusion that the tapping of telephones is therefore illegal would plainly be superficial in the extreme. The reason why a search of premises which is not authorised by law is illegal is that it involves the tort of trespass to those premises: and any trespass, whether to land or goods or the person, that is made without legal authority is prima facie illegal. Telephone tapping by the Post Office, on the other hand, involves no act

126 Id. at 631.
128 Nathan Carrington was the most senior of the “King’s Messengers,” four of whom had conducted the search of Entick’s premises and been sued for trespass in the Court of Common Pleas. Id. at 807–08.
129 Id. at 818.
130 Malone, 2 All E. R. at 640.
of trespass. . . . [A]ll that is done is done within the Post Office’s own domain.131

Vice-Chancellor Megarry was also unwilling to accept Malone’s Fourth Amendment-based argument in support of the existence of an English common law right of telephone privacy. He acknowledged that the Fourth Amendment was “mainly based on the English cases on general warrants, especially Entick v. Carrington.”132 He also recognized that in Katz v. United States, the U.S. Supreme Court had “rejected previous authority which held that the Fourth Amendment was not violated by telephone tapping which was effected without any act of trespass or any seizure of any material object.”133 Nevertheless, he insisted that “[t]hough mainly based on the English cases on general warrants, the Fourth Amendment goes far beyond anything to be found in those cases; and Katz is explicitly based on the Fourth Amendment.”134 He concluded, therefore, that he did not think that “either the Fourth Amendment or the [Katz] decision gives any real assistance to counsel’s contentions for the plaintiff about the law of England.”135

Megarry was also unconvinced by Malone’s argument that Article 8 of the ECHR conferred “direct rights” on U.K. citizens, or at least that it should guide domestic courts in the task of interpreting and applying English law. He held—and on this question he was clearly right at the time—that the Convention “[d]id not, as a matter of English law, confer any direct rights on the plaintiff that he can enforce in the English courts.”136 On use of the ECHR to assist the court in identifying the content of English law, Megarry conceded that “if the question before me were one of construing a statute enacted with the purpose of giving effect to obligations imposed by the convention, the court would readily seek to construe the legislation in a way that would effectuate the convention

131 Id. Megarry’s reasoning is of course strikingly reminiscent of that expressed by Chief Justice Taft’s majority opinion in Olmstead v. United States. See supra notes 16–19 and accompanying text.
132 Malone, 2 All E. R. at 631 (quoting 8 HALSURY’S LAWS OF ENGLAND ¶ 843 (4th ed. 2004)).
133 Id. at 632.
134 Id. at 644.
135 Id.
136 Id. at 647.
rather than frustrate it."\textsuperscript{137} However, Megarry found, “no relevant legislation of that sort is in existence,” and where Parliament has abstained from legislating on a point that is plainly suitable for legislation, it is indeed difficult for the court to lay down new rules of common law or equity that will carry out the Crown’s treaty obligations, or to discover for the first time that such rules have always existed.\textsuperscript{138}

Megarry concluded by revisiting the question of whether the absence of statutory controls, as such, rendered the practice of telephone tapping in Britain unlawful. He alluded to the fact that earlier in his opinion he had held that

\begin{quote}
[i]f the tapping of telephones by the Post Office at the request of the police can be carried out without any breach of the law, it does not require any statutory or common law power to justify it: it can lawfully be done simply because there is nothing to make it unlawful.\textsuperscript{139}
\end{quote}

He concluded that now that he had “held that . . . tapping can indeed be carried out without committing any breach of the law, the contention [that the absence of any grant of powers to the executive renders telephone tapping unlawful] necessarily fails.”\textsuperscript{140}

\begin{footnotes}
\item[137] \textit{Id.} at 647–48.
\item[138] \textit{Id.} at 648. Here—and earlier at pp. 635–38—Megarry devoted considerable attention to the ECHR, to the G10 statute, and to the ECtHR’s decision in the \textit{Klass} case. He noted that “[n]ot a single one of [the] safeguards [contained in the G10 statute] is to be found as a matter of established law in England,” and that “it is impossible to read the judgment in the \textit{Klass} case without it becoming abundantly clear that a system which has no legal safeguards whatever has small chance of satisfying the requirements of [the ECHR].” \textit{Id.} He then remarked that the absence of statutory safeguards rendered telephone tapping “a subject which cries out for legislation.” \textit{Id.} at 649.
\item[139] \textit{Id.} at 638.
\item[140] \textit{Id.} at 649.
\end{footnotes}
4. The Aftermath of Malone

In response to Vice-Chancellor Megarry’s judgment in *Malone*, the Home Secretary addressed Parliament.141 He stated that the government had considered “with great care” Vice-Chancellor Megarry’s suggestion that the use of interception should be governed by legislation.142 However, he went on to say that in the view of the government the interception of communications is, by definition, a practice that depends for its effectiveness and value upon being carried out in secret, and cannot therefore be subject to the normal processes of parliamentary control. Its acceptability in a democratic society depends on its being subject to ministerial control, and on the readiness of the public and their representatives in Parliament to repose their trust in the Ministers concerned to exercise that control responsibly. . . . The Government have come to the clear conclusion that [existing] procedures, conditions and safeguards [are] a good and sufficient protection for the liberty of the subject, and would not be made significantly more effective for that purpose by being embodied in legislation. The Government have accordingly decided not to introduce legislation on these matters.143

Malone responded to his defeat in the High Court by submitting an application to the European Commission of Human Rights.144 On December 17, 1982, the Commission declined to assess the merits of Britain’s non-statutory arrangements for authorization and oversight of wiretapping and held instead that the British system failed to satisfy the “threshold”

---

142 Id. col. 207.
143 Id.
144 Prior to 1998, applications alleging a violation of rights protected by the ECHR were initially submitted to the European Commission, a body consisting of lawyers but not necessarily judges. An applicant could not appeal an adverse decision of the Commission, but the Commission itself could refer a case to the ECtHR (and could do so irrespective of the direction of its decision). In 1998, the Commission was abolished and applications are now submitted directly to the European Court. See ECHR, ECHR OVERVIEW: 1959–2015, at 10, available at http://www.echr.coe.int/Documents/Overview_19592015_ENG.pdf.
requirement of Article 8(2) of the ECHR that any interference with privacy rights protected by Article 8(1) must be “in accordance with the law.”

5. The European Court of Human Rights Decision

On May 16, 1983, the European Commission referred the Malone case to the European Court of Human Rights. Like the European Commission, the ECtHR declined to assess the merits of Britain’s non-statutory interception regime, and held instead that it violated Article 8 because it was “not in accordance with the law.” At the same time, the court elected to use the case as a vehicle for setting forth substantial components of what would become an oft-repeated body of “black letter law” on secret surveillance.

The court first asserted what was obvious: that the ECHR required, at a minimum, that any national system of authorization and oversight of interception of communications “must have some basis in domestic law.” It promptly stiffened this basic requirement, however, by articulating two additional features that it would henceforth regard as essential for purposes of assessing interception legislation. “Firstly,” the court said,

the law must be adequately accessible: the citizen must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case. Secondly, a norm cannot be regarded as “law” unless it is formulated with sufficient precision to enable the citizen to regulate his conduct: he must be able—if need be with appropriate advice—to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail.

---

147 Id. paras. 66–80.
The court conceded that “the requirement of foreseeability cannot mean that an individual should be enabled to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly.” Nevertheless, the court said,

the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence.

The court then wrapped up its articulation of the “general principles” relevant to deciding whether a government’s system of interception of communications would qualify as being “in accordance with the law.” Since the implementation of measures of secret surveillance is “not open to scrutiny by the individuals concerned or the public at large,” the court held that

it would be contrary to the rule of law for the legal discretion granted to the executive to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent 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.

When the foregoing principles were applied to the practice of telephone tapping in Britain, the outcome was predictable. The ECtHR concluded that in England and Wales the law


152 Id.

153 Id. para. 68.

154 Widespread belief that the ECtHR would condemn the practice of telephone tapping in Britain for failing to satisfy the requirement that any interference with privacy rights must be “in accordance with the law” dates at least from Vice-Chancellor Megarry’s 1979 decision in Malone. See supra note 138 and accompanying text.
does not indicate with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities. To that extent, the minimum degree of legal protection to which citizens are entitled under the rule of law in a democratic society is lacking [and therefore] the interferences with the applicant’s right under Article 8 to respect for his private life and correspondence . . . were not “in accordance with the law.”

6. Interception of Communications Act 1985

The ECtHR’s decision in Malone finally prompted the British government to enact legislation. However, what the court had decided in Malone was that the practice of interception of communications in Britain failed to satisfy the threshold requirement that any interference with Article 8 privacy rights must be “in accordance with the law.” This decision was based, in turn, solely on the fact that existing arrangements for intercepting communications had not been embodied in a written law. The government decided to take advantage of the limited scope of the court’s decision by requesting that Parliament give statutory expression, albeit with some important modifications, to the status quo.

The Interception of Communications Act 1985 made it a crime to intentionally “intercept a communication in the course of its transmission by post or by means of a public telecommunication system.” However, a person was not guilty of an offense if “the communication is intercepted in obedience to a warrant issued by the Secretary of State.”

Section 2 of the Act then granted the Secretary of State the power to issue interception warrants. The Act prescribed that the Secretary of State “shall not issue a warrant . . . unless he considers that the warrant is necessary (a) in the interests of national security; (b) for the purpose of preventing or
detecting serious crime; or (c) for the purpose of safeguarding the economic well-being of the United Kingdom.\textsuperscript{161}

Requests for warrants to conduct internal or domestic wiretapping and other forms of covert surveillance originate primarily with the police and the Security Service (MI5) and are submitted for approval to the Secretary of State for the Home Department.\textsuperscript{162} According to the initial report of Lord Lloyd, the first Interception of Communications Commissioner, the basic procedure for the issuance of a warrant is that

[w]hen an application arrives at the Home Office (I take the Home Office as typical) it is processed by the Warrants Unit . . . to ensure that the application is in order, and that the grounds put forward come within Section 2(2) of the Act. If there is any doubt, the application is referred back. If the application is approved . . . it is referred to the Permanent Under Secretary [and only then] is put before the Home Secretary for his personal approval.\textsuperscript{163}

The 1985 Act crafted two mechanisms, in addition to the warrant process itself, to oversee interception of communications by law enforcement and intelligence-gathering officials. First, the Act established the position of Interception of Communications Commissioner and specified that the Commissioner would be appointed by the Prime Minister and would be “a person who holds or has held a high judicial office.”\textsuperscript{164} The three principal responsibilities of the Commissioner were (1) “to keep under review the carrying out by the Secretary of State of the functions conferred upon him by [the 1985 Act],”\textsuperscript{165} (2) to respond to requests for assistance from the

\textsuperscript{161} Id. § 2(2).
\textsuperscript{162} Other secretaries of state—e.g., the Foreign Secretary and the Defence Secretary—are also authorized to issue warrants. In particular, requests from GCHQ to conduct external or strategic surveillance are ordinarily submitted to the Foreign Secretary. See INTERCEPTION OF COMMUNICATIONS COMMISSIONER, REPORT, 2011–12, H.C. 496, at 5, 16 (U.K.).
\textsuperscript{164} ICA 1985, supra note 158, § 8(1).
\textsuperscript{165} Id. § 8(1)(a).
Interception of Communications Tribunal, and (3) to make an annual report to the Prime Minister.

Commissioners soon adopted two practices. First, they began examining a random sample of warrants issued by the Secretary of State. Second, they paid regular visits to the police, the intelligence services, and the other agencies authorized to apply to the Secretary of State for interception warrants. The findings from these inspections and visits are presented in an annual report to the Prime Minister.

The second oversight mechanism established by the 1985 Act was the Interception of Communications Tribunal. The tribunal was comprised of “five members each of whom shall be a barrister, advocate or solicitor of not less than ten years’ standing.” It was charged with investigating applications from “[a]ny person who believes that communications sent to or by him have been intercepted.” In fulfilling this task, the tribunal was instructed to investigate “whether there is or has been a relevant warrant,” and, where such a warrant exists, to investigate “whether there has been any contravention of sections 2 to 5 [of the Act].”

The tribunal was next instructed that when it investigates a complaint, it should apply “the principles applicable by a court on an application for judicial review.” British courts at the time possessed the power of

---

166 Id. § 8(1)(b). For further discussion of the role of the tribunal, see infra notes 169–85 and accompanying text.
169 ICA 1985, supra note 158, § 7, sch. 1(1).
170 Id. § 7(2). The tribunal was authorized to decline to investigate any application “appearing to the Tribunal to be frivolous or vexatious.” Id. § 7(3).
171 Id. § 7(3)(a).
172 Id. § 7(3)(b). Sections 2 to 5 set forth in detail the process to be followed by the Secretary of State when issuing interception warrants.
173 Id. § 7(4).
“judicial review of administrative action,” that is, the power to declare *ultra vires* the decisions of executive and administrative officials on whom Parliament, by law, had conferred decision-making power. There were numerous relatively specific grounds on which a court could overturn an official’s decision, but it was also theoretically possible to do so on the residual ground that the decision was “unreasonable.”

In a case decided in 1947, however, Lord Greene of the Court of Appeal articulated a remarkably lenient definition of “unreasonable.”\(^{174}\) According to Lord Greene, a court could invalidate the decision of an executive or administrative official, but only if the court was convinced that the decision was “so unreasonable that no reasonable [decision maker] could ever have come to it.”\(^{175}\) Lord Greene’s definition gained wide acceptance and thereafter became known as “Wednesbury unreasonableness.”\(^{176}\)

In the context of interception of communications, the statutory instruction to apply “the principles applicable by a court on an application for judicial review” meant that the tribunal was prohibited from overturning the decision of the Secretary of State to issue an interception warrant unless it believed that the decision was “so unreasonable that no reasonable Secretary of State could ever have come to it.”\(^{177}\) In addition, as we have seen, the Act authorized the issuance of warrants to achieve three broadly defined sets of goals: to protect national security, to prevent or detect serious crime, and to safeguard the economic well-being of the United Kingdom.\(^{178}\) Finally, the Act conferred on the Secretary of State subjective discretion to issue a warrant whenever “he considers that the warrant is necessary” to achieve these goals. The predictable result was that numerous commentators expressed serious doubts about the efficacy of the tribunal as a check on the Secretary of State’s exercise of executive power.\(^{179}\)


\(^{175}\) Id. at 234.


\(^{177}\) See supra notes 173–75 and accompanying text.

\(^{178}\) See ICA 1985, supra note 158 and accompanying text.

In fact, doubts about the degree to which the 1985 Act realistically addressed the problem of executive power to engage in telephone tapping went beyond skepticism about the tribunal’s ability to strictly scrutinize the Secretary of State’s decisions. The Act instructed the tribunal that if it concluded that sections 2 to 5 of the Act had been contravened, it was to “give notice to the applicant” and to “make a report” to the Prime Minister.\textsuperscript{180} If, on the other hand, the tribunal were to “come to any [other] conclusion,” it was instructed to “give notice to the applicant stating that there has been no contravention of [sections 2 to 5 of the Act] in relation to a relevant warrant.”\textsuperscript{181} Such “notice,” of course, would not inform the applicant whether his communications had or had not been intercepted, only that, if they had been, the Secretary of State’s decision to issue a warrant had not, in the opinion of the tribunal, been “Wednesbury unreasonable.” For any applicant other than one against whom the Secretary of State had grossly misused his statutory power, the trip to the tribunal was therefore both fruitless and uninformative.\textsuperscript{182}

To ensure, moreover, that the tribunal was the final stop for applicants believing themselves to be under surveillance, the 1985 Act prescribed that the tribunal’s decision “shall not be subject to appeal or liable to be questioned in any court.”\textsuperscript{183} This prohibition on judicial review of the tribunal’s decisions by an ordinary court was intended to insulate the decisions of the tribunal from further scrutiny unless an individual decision of the tribunal, or the \textit{modus operandi} of the tribunal itself, was successfully challenged in the ECtHR.

Finally, there was the question of whether someone whose communications had been intercepted could or would learn by any other means whether an interception had occurred. On this issue, the 1985 Act

\textsuperscript{180} ICA 1985, \textit{supra} note 158, § 7(4).

\textsuperscript{181} Id. § 7(7).

\textsuperscript{182} After the passage of RIPA 2000, the Interception of Communications Tribunal was replaced by the Investigatory Powers Tribunal (IPT). RIPA now forbids the Secretary of State from issuing an interception warrant unless he believes not only that the warrant is “necessary,” but also that “the conduct authorized by the warrant is proportionate to what is sought to be achieved by that conduct.” RIPA 2000, \textit{supra} note 157, § 5(2). As a result, the IPT is now obliged to evaluate the Secretary of State’s decision on the basis of both its “necessity” and its “proportionality,” rather than its mere avoidance of “Wednesbury unreasonableness.” See infra note 230 and accompanying text. That said, the IPT remains “confined” to giving notice to a complainant either that it has “made a determination in his favour [or] that no determination has been made in his favour.” RIPA 2000, \textit{supra} note 157, § 68(4).

\textsuperscript{183} ICA 1985, \textit{supra} note 158, § 7(8).
prescribed that “[i]n any proceedings before any court or tribunal”—apart from the Interception of Communications Tribunal itself, whose proceedings were ordinarily closed both to the applicant and to his or her legal representative—“no evidence shall be adduced and no question in cross-examination shall be asked which . . . tends to suggest . . . that an offence [under section 1 of the Act] has been committed [e.g., by a government official, a police officer, or a public telecommunications operator] or . . . that a warrant has been or is to be issued to any of those persons.”\footnote{ICA 1985, supra note 158, § 9(1).} Thus, the Act gave statutory force to the Home Office policy of refusing to rely on intercept evidence in judicial proceedings and refusing to confirm or deny whether interception had ever occurred.\footnote{See supra note 114 and accompanying text. RIPA 2000 perpetuates the total exclusion of interception evidence from criminal trials and other public proceedings. See RIPA 2000, supra note 157, § 17.}

7. The Interception of Communications Act and Individual Rights

From an American perspective, it is easy to see why civil libertarians and other commentators in the United Kingdom viewed the Interception of Communications Act 1985 with consternation and alarm. The legislation constituted statutory recognition of the power of the state to engage in interception of postal and telephone communications. However, it located the power to issue interception warrants exclusively in the person of the Secretary of State. Moreover, it authorized the Secretary to issue warrants in three broad categories of circumstances whenever he considered it “necessary” to do so. The Act conferred general oversight responsibility on a figure who was required to hold or have held “high judicial office” but who was appointed by, and reported to, the Prime Minister. It established a tribunal consisting of senior members of the legal profession to which an individual who believed himself or herself to have been under surveillance could apply. However, it authorized the tribunal to conduct its deliberations without the participation of the applicant or his or her legal representative. Moreover, it instructed the tribunal to reach conclusions about the legality of an interception warrant by asking itself whether the Secretary of State’s decision to issue the warrant had been one that was “so unreasonable that no reasonable Secretary of State could ever have come to it.”\footnote{Cf. supra note 175 and accompanying text.} Finally, it instructed the tribunal to inform an applicant—either one whose
communications had not been intercepted or one whose communications had been intercepted, in the opinion of the tribunal, pursuant to a lawfully issued warrant—that there had been “no contravention” of the statutory provisions governing the issuance of warrants.

In addition to the foregoing features, the 1985 Act contained other glaring departures from the widely held belief, at least among legal scholars and civil libertarians, that courts should play a key role in approving or at least in reviewing executive branch decisions to engage in interception of communications. The Act endeavored to make the tribunal the exclusive forum in which citizens could challenge suspected governmental interception of postal or telephone communications by prescribing that decisions of the tribunal “shall not be subject to appeal or liable to be questioned in any court.” In addition, the Act forbade any use of interception evidence in court or any reference in court to the fact that interception had occurred. The obvious question that arose at the time of the Act’s passage was whether it could possibly satisfy the requirements of Article 8 of the ECHR. The prevailing view, at the time, was that it could not.187

B. The Run-up to RIPA, 1985–2000

Parliament’s decision to go no further than to give statutory expression to the status quo was regarded by many as an inadequate response to the ECtHR’s insistence that the British government adopt legislation to govern the use of wiretapping. In addition, it was widely recognized that forms of covert surveillance other than wiretapping continued to be exempt from statutory regulation. Lastly, none of Britain’s principal intelligence agencies—the Security Service (MI5), the Secret Intelligence Service (MI6), and the Government Communications Headquarters (GCHQ)—were subject to statutory control. Predictably, political pressure began to build within Britain to eliminate these glaring gaps in the coverage of the written law.

187 See, e.g., Leigh, supra note 179, at 18 (noting “there is nothing in the [1985] Act which gives any cause to believe that the rights of the individual have been significantly safeguarded against arbitrary interference by the State.”); Zellick, supra note 179, at 308 (arguing portions of the 1985 Act demonstrate the British government “is not fully subject to the law”); Cameron, supra note 179, at 149 (arguing the 1985 Act is at most a “minimalist interpretation of the United Kingdom’s obligations under the European Convention on Human Rights”); Lloyd, supra note 179, at 94 (noting “it may be doubted” whether the provisions of the 1985 Act meet the requirements of the ECHR). See also infra notes 215–23, 234–72 and accompanying text.

The Security Service (MI5) was founded in 1909 and is responsible today for responding, within Britain, to domestic and foreign threats to national security. In 1937, the government determined that the Security Service, along with the police, should secure a warrant from the Secretary of State for the Home Department before engaging in wiretapping. The criteria for issuance of a warrant were first published in the Birkett Report, and they included the stipulation that the Secretary of State should not issue a warrant to the Security Service unless there is “a major subversive, terrorist or espionage activity that is likely to injure the national interest.”

Catherine Massiter worked in MI5 from 1981 to 1983. In 1985, she went public with a set of damning allegations about the way the non-statutory warrant-granting process in national security cases functioned during her employment with the agency. In particular, Massiter made three specific claims, each of which was based on her personal knowledge: first, she alleged that the Secretary of State had issued a warrant of questionable legality to wiretap the telephone of John Cox, a long-time member of the British Communist Party who was also an official of the Campaign for Nuclear Disarmament, Britain’s leading anti-nuclear peace group. Second, she alleged that MI5 maintained files on Patricia Hewitt and Harriet Harman, two officials of the National Council for Civil Liberties, which at the time was Britain’s most prominent civil liberties group. Finally, she alleged that as a by-product of the wiretap on John Cox’s telephone, MI5 classified Hewitt and Harman as “communist sympathisers” and had included in their

---

188 The Security Service acquired its enduring, if unofficial, title of “MI5” when, in 1916, the then seven-year-old Secret Service Bureau was incorporated into the new Directorate of Military Intelligence. See Christopher Andrew, Defend the Realm: The Authorized History of MI5, at 3–28 (2009).

189 See supra notes 107–13 and accompanying text.

190 Birkett Report, supra note 98, ¶ 67.

191 Margaret Thatcher became Prime Minister in 1979. Massiter’s employment with MI5 thus coincided with the early years of the Thatcher Government.

192 Massiter’s allegation is detailed in affidavits provided to the High Court in a legal challenge to the Secretary of State’s decision to issue a warrant. The case was brought by Cox and two other officials of the Campaign for Nuclear Disarmament with whom Cox spoke by phone on a regular basis. R. v. Sec’y of State for the Home Dep’t, ex parte Ruddock, [1987] 2 All E.R. 518 (Q.B.).

files information about their personal lives, their political opinions, and their professional activities.\textsuperscript{194} Based on Massiter’s allegations, John Cox and two colleagues requested judicial review in the High Court of the legality of the Secretary of State’s decision to issue an interception warrant. Judge Taylor’s decision in the case was issued shortly after passage of the Interception of Communications Act 1985.\textsuperscript{195} Taylor noted that the Act conferred jurisdiction to investigate complaints of unlawful wiretapping on the Interception of Communications Tribunal, and that the courts would “henceforth cease to have any supervisory or investigatory function in the field of interceptions.”\textsuperscript{196}

However, Taylor declined to accept the government’s argument that the present litigation was “merely academic.”\textsuperscript{197} Instead, he asserted that “[i]f wrongdoing were proved”—that is, if the Secretary of State had issued a warrant in contravention of the government’s non-statutory guidelines—“the court should [not] shrink from declaring [that fact].”\textsuperscript{198} The government adhered to its policy of neither confirming nor denying that wiretapping had occurred but submitted an affidavit assuring the court that “no warrant has been issued which has not complied [with the existing non-statutory criteria requiring the existence of a ‘major subversive activity’].”\textsuperscript{199} On the basis of the government’s assurance, and without holding any sort of hearing, Taylor concluded that the Secretary of State’s decision to issue a warrant had not been “Wednesbury unreasonable,” and that therefore “these applications must be refused.”\textsuperscript{200}

Three years later, the European Commission resolved Hewitt and Harman’s claim that the Security Service had improperly collected and retained information on their beliefs and activities.\textsuperscript{201} Since its inception, the Security Service had not been governed by parliamentary legislation.\textsuperscript{202} As a


\textsuperscript{195} The legislation had taken effect on April 10, 1986.

\textsuperscript{196} Ruddock, supra note 192, at 528.

\textsuperscript{197} Id.

\textsuperscript{198} Id.

\textsuperscript{199} Id. at 524. See supra note 112 and accompanying text.

\textsuperscript{200} Ruddock, supra note 192, at 534–35.


result, the Commission held that the interference with the applicants’ rights under Article 8(1) “was not ‘in accordance with the law’ as required by Article 8(2),” and that therefore the United Kingdom was in breach of its obligations under the ECHR.203

2. The Security Service Act 1989 and the Intelligence Services Act 1994

In a resolution adopted in the wake of the European Commission’s decision in Hewitt and Harman, the Committee of Ministers of the Council of Europe noted that it had been “informed by the Government of the United Kingdom that the Security Service Act 1989 came into force on 18 December 1989.”204 To satisfy the ECHR’s requirement that any interference with rights must be “in accordance with the law,” the Security Service Act placed the Security Service on a statutory footing, subject to the authority of the Secretary of State for the Home Department.205 In addition, following the template introduced by the Interception of Communications Act 1985, the Act created a Security Service Commissioner and a Security Service Tribunal.206

The Security Service Act 1989 did not change the status quo with regard to wiretapping. Since 1937, the Security Service had been obliged to seek warrants from the Secretary of State before engaging in such surveillance, and this arrangement was placed on a statutory footing when Parliament passed the Interception of Communications Act in 1985. The principal innovation of the 1989 Act was to establish a system whereby the Security Service was also obliged to seek warrants from the Secretary of State for “entry on or interference with property,”207 that is, for operations in which there was entry to property either to seize or photograph items or to install a listening device.208

The transformation of the United Kingdom’s security and intelligence agencies was taken a step further with Parliament’s passage of the Intelligence Services Act 1994. The Act placed Britain’s other two principal intelligence agencies—the Secret Intelligence Service (MI6) and the

---

204 Id. at 668–69. At the time, the Committee of Ministers was the body responsible for enforcing the decisions of the European Commission and the ECtHR.
205 Security Service Act 1989, c.5, § 1(1).
206 Id. §§ 4–5.
207 Id. § 3(1).
208 See Lustgarten & Leigh, supra note 11, at 72–79; Andrew, supra note 188, at 753–68.
Government Communications Headquarters (GCHQ)—on a statutory footing.\textsuperscript{209} These agencies, like the Security Service, were made subject to the authority of the Secretary of State, from whom they were required to obtain a warrant before undertaking any “entry on or interference with property.”\textsuperscript{210} Pursuant to the Interception of Communications Act 1985, the agencies also remained obligated to seek a warrant from the Secretary of State before engaging in wiretapping.

3. The Labour Government and Policy Change

The election of a Labour government headed by Tony Blair in 1997 brought to a head a number of policy debates anchored in concerns about the United Kingdom’s embarrassing defeats in Strasbourg, and the haphazard process by which Parliament and the courts had been addressing the status of secret surveillance.\textsuperscript{211} The government responded by announcing its intention to introduce in Parliament not only a “Human Rights Act”—the purpose of which would be to “incorporate” the ECHR into British law—but also comprehensive legislation to govern the authorization and use by government officials of not only telephone wiretapping but also other forms of covert surveillance.\textsuperscript{212} In November 1998, Parliament passed the Human Rights Act, and scheduled it to take effect in October 2000.\textsuperscript{213} In February 2000, Parliament began consideration of the Regulation of Investigatory Powers Act 2000, the government’s proposed comprehensive surveillance legislation.\textsuperscript{214}

As was customary, the government invited public feedback on the content of the new legislation. Submissions were received from various sources, including pressure groups dedicated to the protection of civil liberties and human rights. The response of the human rights organization Liberty was

\textsuperscript{209} Intelligence Services Act 1994, c. 13, §§ 1, 3.
\textsuperscript{210} Id. §§ 5(1)–(2).
\textsuperscript{212} Nick Taylor, State Surveillance and the Right to Privacy, 1 SURVEILLANCE & SOCIETY 66 (2002).
typical. The group strenuously opposed retention of the system of executive warrants given statutory expression in the Interception of Communications Act 1985. Liberty pointed out that while RIPA represented “an improvement on the existing law,” it failed to recognize that “the case law of the European Convention on Human Rights emphasises that prior judicial sanction is the preferable safeguard for the citizen’s Article 8 privacy rights in the investigative context.”

4. The RIPA Debate in Parliament

Responsibility for defending the merits of RIPA in Parliament fell to the Home Secretary, Jack Straw. Early in the debate, Straw was asked by Simon Hughes, the chief spokesperson for the Liberal Democratic Party, whether he could explain “why . . . the opportunity [was] not taken to do what many democratic countries have done, and transfer the [power to authorise interception of communications] from politicians or officials to a judicial authority in the first instance?” In response, the Home Secretary made several points. First, he assured Parliament that “[t]he powers that are exercised by the Secretary of State—certainly by me and, I believe, by every one of my predecessors—have been exercised very carefully.” Second, he argued that “the system is judicially supervised,” because the Interception of Communications Commissioner, who engages in ex post review of a random sample of the Secretary of State’s decisions to issue a warrant, “is someone of high judicial standing.” Finally, he argued that:

If one looks at the practice in other countries, it does not necessarily follow that, just because a judicial warrant is required, there is a greater safeguard for the individual. Indeed, I suggest that, in quite a number of other countries, the fact that a judicial warrant is required lessens the protection that is

---

216 Id.
218 Id. col. 769.
219 Id. col. 770.
220 Id.
offered to people because the judicial warrant acts as a fig leaf for people’s human rights, and not as a serious safeguard.221

When the debate moved to the House of Lords, discussion of executive versus judicial pre-approval of interception warrants continued. Addressing a specific set of amendments intended to locate the power to issue warrants in a judge, rather than the Secretary of State, the spokesperson for the Liberal Democratic Party, Lord Phillips of Sudbury, took a conciliatory tone. He cautioned that he was not suggesting that “the Secretary of State is ‘unfit’ . . . to undertake the task [of issuing interception warrants].” Nevertheless, he said, “a considerable body of informed opinion in the country now believes that this task would be better undertaken by a judge.”222 The government’s spokesperson, Lord Bach, replied that

[t]he arguments put forward by those who advocate judicial involvement do not at the end of the day persuade the Government that that is the right course to take. We maintain the view that authorising interception involves particularly sensitive decisions that are properly a matter for the executive. . . .

Of course, there is an important, vital place for judicial involvement. That comes . . . in the independent judicial oversight provided by the commissioners and the tribunal, who are there to provide a remedy if the executive has acted outside its statutory powers.223

As the debate drew to a close, the Liberal Democratic Party stood alone in opposing the government’s decision to retain in the hands of the Secretary of State the power to issue interception warrants.224 On July 26, 2000, RIPA was enacted. Two days later it received the Royal Assent, and on October 2, in tandem with the Human Rights Act 1998, it took effect.225

221 Id.
223 Id. col. 1487.
224 Id. cols. 1491–92.

In RIPA 2000, Parliament fulfilled the Blair government’s promise to enact into law a comprehensive regime for the regulation of surveillance-based investigatory powers. RIPA perpetuated existing arrangements for the regulation of telephone tapping. In addition, RIPA established rules for the acquisition and disclosure of “communications data” and incorporated previous legislation subjecting to statutory control “entry on or interference with property” by the security and intelligence agencies and the police. Finally, the legislation prescribed rules for the use by various public agencies of additional types of “covert surveillance,” including “intrusive surveillance,” “directed surveillance,” and the deployment of “covert human intelligence sources.”

RIPA repealed the Interception of Communications Act 1985, and replaced it with fresh provisions governing the interception of postal and telephone communications. However, the interception provisions of RIPA were nearly identical to those of the earlier law, albeit with some potentially significant modifications. First, in keeping with long-standing doctrine of the ECtHR, RIPA augmented the requirement that the Secretary of State shall not issue an interception warrant unless he believes it is “necessary” to do so with a requirement that he must also believe “that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct.” Second, the law mandated the promulgation of “Codes of Practice” designed to provide the police and intelligence agencies with practical guidance regarding “the exercise and performance of the powers and duties mentioned [in the Act].” Finally, RIPA created a single Investigatory Powers Tribunal (IPT) to assume the duties of the Interception of Communications Tribunal, the Security Service Tribunal, and the Intelligence Services Tribunal. The IPT was given jurisdiction “to investigate any event that you believe has taken place against you, your

---

230 Id. § 5(2)(b).
property or your communications, as long as it relates to the use of a covert
technique by a public authority regulated under [RIPA 2000] or a wider
human rights breach by the intelligence agencies."232

6. Conclusion

In the decade and a half after 1985, the legal landscape relating to the
British government’s use of electronic surveillance and other investigatory
powers was transformed. By 1994, all three of the principal intelligence
agencies—MI5, MI6, and GCHQ—had been placed on a statutory footing,
and their power to engage in various forms of covert surveillance had been
subjected to statutory control. In 1997, Parliament enacted statutory
provisions to govern police interference with property for the purpose of
installing a listening device.233 In RIPA 2000, Parliament merged these and
other earlier changes into a comprehensive statutory regime to govern the use
of a broad spectrum of surveillance techniques by a variety of public bodies,
including, but not limited to, the police and the intelligence agencies.

Virtually every one of the foregoing statutory developments was
prompted by a successful or pending challenge to the status quo on the part
of litigants who had invoked the enforcement mechanisms of the ECtHR.
The reactive nature of the legislative policies enacted between 1985 and
2000 has fueled continuing skepticism among civil libertarians and other
commentators about the merits of British surveillance arrangements.234
There is dismay that the British government has not introduced a system of
judicial pre-approval of interception of communications, at least in
connection with ordinary criminal investigations.235 There is also alarm at
the care with which the government has succeeded in engineering the
exclusion of ordinary courts from any role in responding to citizens’
complaints.236 Finally, there is a lingering suspicion that the net effect of
Parliament’s legislative responses to ECtHR decisions has been to diminish

233 Police Act 1997, c. 50, § 93.
234 See supra note 187 and accompanying text.
235 See, e.g., Helen Fenwick, Civil Liberties and Human Rights 1098 (4th ed. 2007) (“Perhaps the most striking feature of the RIPA is the determination evinced under it to
prevent citizens invoking Convention rights in the ordinary courts against State bodies in
respect of the profound threat to privacy represented by interception and surveillance.”).
rather than to enhance citizens’ rights. What is undeniable is that in a relatively brief fifteen year period Parliament succeeded in passing an impressive body of statutory law designed to shield Britain from further embarrassing losses in the ECtHR, and to respond, however grudgingly, to the requirement of Article 8(2) of the ECHR that any interference with Article 8(1) privacy rights must be both “in accordance with the law” and “necessary in a democratic society.”

IV. RIPA 2000 IN THE EUROPEAN COURT: THE KENNEDY CASE

The passage of RIPA 2000 set the stage for a judgment by the ECtHR on whether the British approach to telephone wiretapping was compatible with Article 8 of the ECHR. The case, Kennedy v. United Kingdom, originated a full twenty years earlier with an incident in which the applicant, Malcolm Kennedy, was arrested for drunkenness and shared an overnight jail cell with another man. When the cellmate was found dead the next morning, Kennedy was charged with murder. Although he alleged that the police were covering up their own responsibility for the death, Kennedy was eventually convicted of manslaughter. Upon his release in 1996, he became convinced that he was the target of illegal telephone tapping by the police, and in 2001, he lodged a complaint with the Investigatory Powers Tribunal. On January 17, 2005, the IPT notified Kennedy that “no determination had been made in his favour.” On July 12, 2005, Kennedy applied to the European Court of Human Rights.

The ECtHR chose to use Kennedy’s complaint to address “the general compliance [with Article 8 of the ECHR] of the RIPA regime for internal communications.” The court was determined, in other words, not to decide whether the applicant’s telephone calls had actually been intercepted,

---

237 See, e.g., Laura K. Donohue, Anglo-American Privacy and Surveillance, 96 J. CRIM. L. & CRIMINOLOGY 1059, 1063 (2006) (“Beginning in the mid-1980s, the European Court began to raise objections to the lack of safeguards and statutory framework. But each time the Court handed down a significant finding against the United Kingdom, the state responded [by expanding executive surveillance authorities.” (emphasis in original)). But see Laura K. Donohue, The Perilous Dialogue, 97 CAL. L. REV. 357, 383 (2009) (“Even recognizing the many limitations of [RIPA], the complex web of oversight mechanisms in the United Kingdom does offer some check on untrammeled executive power—protections that for the most part do not exist in the United States.”).


239 Id. para. 20.

240 Id. para. 109.
and, if they had been, whether the interception was lawful. Instead, it signaled its intention to assess the “facial validity” of the provisions of RIPA that govern the interception of non-international telephone and postal communications. Incorporated in this assessment was the question of whether the procedures followed by the Investigatory Powers Tribunal in addressing individual complaints were compatible with Article 6 of the ECHR, which guarantees that “everyone is entitled to a fair and public hearing [by] an independent and impartial tribunal established by law.”

A. The Article 8 Complaint

The ECtHR prefaced its assessment of the facial validity of RIPA by summarily rejecting the government’s argument that Kennedy lacked standing to bring the case. According to the court, Kennedy could challenge RIPA because he had brought his complaint “on the basis of the very existence of measures permitting secret surveillance.”

The court then addressed various specific objections to the surveillance regime established by the Interception of Communications Act 1985 and perpetuated in RIPA 2000. First, the court concluded that the terms “national security” and “serious crime”—the broad grounds on which the Secretary of State is authorized to base decisions to issue interception warrants—were sufficiently clear to satisfy the court’s “foreseeability” requirement. The court expressly held that interception legislation is not required “to set out exhaustively by name the specific offences which may give rise to interception.” In addition, the court upheld the Convention-compatibility of RIPA’s provisions on the duration of interception warrants and on the procedures for “examining, using and storing data” and other components of the process of dealing with the product of an interception order.

In response to the absence of any mechanism in RIPA for judicial pre-approval of surveillance requests—and in light of its own oft-repeated assertion that in the area of secret surveillance, “it is in principle desirable to

---

241 ECHR, supra note 9, art. 6(1).
245 Id. paras. 161–165.
entrust supervisory control to a judge—\(^{246}\) the ECtHR warmly endorsed the role of the Interception of Communications Commissioner. The court described the Commissioner as a person who “holds or has held high judicial office,” who is “independent of the executive and the legislature,” and who in the exercise of his responsibilities “provides an important control of the activities of the intercepting agencies and of the Secretary of State himself.”\(^ {247}\)

With respect to the Investigatory Powers Tribunal, the sole domestic forum authorized to entertain complaints of unlawful surveillance, the court described the IPT as “an independent and impartial body,” and noted that it was composed of persons who “hold or have held high judicial office or [are] experienced lawyers.”\(^ {248}\) The court also emphasized the IPT’s accessibility, noting that it is a body to which “any person who suspects that his communications have been or are being intercepted may apply,” irrespective of whether they have been notified of that fact.\(^ {249}\) Finally, the court noted that there was “no evidence of any significant shortcomings in the application and operation of the surveillance regime.”\(^ {250}\) It concluded that

\[
\text{having regard to the safeguards [offered] by the supervision of the Commissioner and the review of the IPT, the impugned surveillance measures, insofar as they may have been applied to the applicant in the circumstances outlined in the present case, are justified under Article 8(2).}^{251}\]

**B. The Article 6 Complaint**

RIPA 2000 established the Investigatory Powers Tribunal and conferred upon it exclusive jurisdiction to entertain complaints from individuals who believe they have been the target of unlawful governmental wiretapping or

\(^{246}\) *Id.* para. 167. The court’s preference for judicial supervision was first enunciated in its decision in *Klass.* See *Klass*, App. No. 58243/00, 28 Eur. Ct. H.R. para.56.


\(^{248}\) *Id.* para. 167.

\(^{249}\) *Id.* para. 169. The court’s purpose in making this point was to signal its willingness to distinguish the way in which RIPA operated in practice from the way in which surveillance was conducted in countries in which statutory controls on executive branch activities were impressive on their face but evidently ignored in practice. For further discussion, see *infra* notes 302–16 and accompanying text.

other forms of covert surveillance. The law also confers on the Secretary of State the power to draft the rules under which the tribunal will operate. In October of 2000, in conjunction with RIPA’s coming into force, the Secretary of State promulgated the Tribunal’s Rules.

The Rules prescribed that when the IPT agrees to investigate an individual complaint, it “may” hold oral hearings, including hearings at which “the complainant may make representations,” but it is under no duty to do so. Further, the tribunal is authorized to hold “separate oral hearings.” Should the tribunal choose to hold a separate hearing to which the government alone is invited, it is authorized to not disclose “to the complainant or to any other person” the fact it has held, or proposes to hold, such a hearing. It is also permitted to not disclose to the complainant or to any other person . . . any information or document disclosed or provided to the Tribunal in the course of that hearing, or the identity of any witness at that hearing.

Finally, the tribunal is instructed that its “proceedings, including any oral hearings, shall be conducted in private.”

Kennedy’s complaint to the IPT had argued that Article 6 of the ECHR required that the tribunal’s proceedings must be adversarial in nature and open to the public. Article 6 guarantees to everyone “a fair and public hearing [by] an independent and impartial tribunal.” Kennedy argued that this required that the tribunal’s proceedings take the form of a public oral hearing with mutual disclosure and inspection of the parties’ evidence, that oral evidence be open to cross-examination, and that “following its final determination, the IPT [should] state its findings and give reasons for its conclusions on each relevant issue.” Most of these requests, of course, were wholly at odds with the constraints under which the tribunal had been instructed to operate by the Secretary of State.

252 RIPA 2000, supra note 157, § 65.
253 Id. § 69(1)(a).
255 Id. art. 9(2)–(4).
256 Id. art. 6(2)(a).
257 Id. art. 6(2)(b).
258 Id. art. 9(6).
259 ECHR, supra note 9, art. 6(1).
The government defended the IPT’s operating procedures on the ground “the overarching consideration was that an individual could not be notified of interception measures while interception was ongoing or where notification would jeopardise the capabilities or operations of intercepting agencies.”\(^{261}\) It reminded the ECtHR that RIPA conferred on the IPT “full powers to obtain any material it considered necessary from relevant bodies,” including the police, the intelligence agencies, and the Secretary of State, and it insisted that “the procedure before the IPT offered as fair a procedure as could be achieved in the context of secret surveillance powers.”\(^{262}\)

The ECtHR prefaced its conclusions on the Article 6 question by noting that in prior decisions it had held that “restrictions on the right to a fully adversarial procedure [were permissible] where strictly necessary.”\(^{263}\) It also “emphasised[d] that [IPT] proceedings related to secret surveillance measures and that there was therefore a need to keep secret sensitive and confidential information.”\(^{264}\) This consideration, the court said, “justifies restrictions in the IPT proceedings.”\(^{265}\) In the court’s view, the question was “whether the restrictions, taken as a whole, were disproportionate or impaired the very essence of the applicant’s right to a fair trial.”\(^{266}\)

The court then turned to specific rules that governed the IPT’s investigation of individual complaints. First, the court considered the tribunal’s strict limitations on the disclosure to the complainant of any information provided to the tribunal, or even disclosure to the complainant of the fact that the tribunal had held, or was proposing to hold, a separate oral hearing to which the government alone would be invited. The court agreed with the government that the alternatives, such as disclosure of redacted documents or the appointment of special advocates, would not solve the problem, because they could not “achieve[] the aim of preserving the secrecy of whether any interception had taken place.”\(^{267}\) The court also agreed with the government that conferring on the tribunal the discretion to refuse to hold oral hearings at all was compatible with Article 6.\(^{268}\) Finally, the court endorsed the government’s strict policy of refraining from

\(^{261}\) Id. para. 182.
\(^{262}\) Id. para. 183.
\(^{263}\) Id. para. 184.
\(^{264}\) Id. para. 186.
\(^{265}\) Id.
\(^{266}\) Id.
\(^{267}\) Id. para. 187.
\(^{268}\) Id. para. 188.
providing post-surveillance notification to any targeted persons, even in criminal investigations, and of neither confirming nor denying, in court or anywhere else, that interception of communications had ever occurred. It held that these goals “could be circumvented if an application to the IPT resulted in a complainant being advised whether interception had taken place. In the circumstances, it is sufficient that the applicant be advised that no determination has been in his favour.”

The court then reached its overall conclusion that “the restrictions on the applicant’s rights in the context of the proceedings before the IPT were both necessary and proportionate and did not impair the very essence of the applicant’s Article 6 rights.”

C. Conclusion

The ECtHR’s decision in *Kennedy* constituted a ringing endorsement of the Convention-compatibility of the RIPA regime for interception of communications in the United Kingdom. RIPA authorizes the government to engage in interception of communications within the United Kingdom in both criminal investigations and intelligence-gathering operations. The Secretary of State for the Home Department is empowered to issue interception warrants to both the police and counter-intelligence officials provided he or she believes that it is “necessary” and “proportionate” to do so in order to accomplish one or more of three broad objectives. The ECtHR upheld the RIPA provisions authorizing executive warrants and endorsed the mechanisms established by RIPA—including the Interception of Communications Commissioner and the Investigatory Powers Tribunal—to oversee the Secretary of State’s exercise of the warrant-granting power. In addition, the court upheld the arrangements for the nearly complete secrecy that surrounds the IPT’s operations in the exercise of its jurisdiction to investigate citizens’ complaints of unlawful surveillance by government officials. The court concluded unanimously that RIPA’s complex and distinctive mix of powers and safeguards rendered the British approach to interception of communications and other forms of covert surveillance

---

269 *Id.* para. 189.
270 *Id.* para. 190.
“necessary in a democratic society” and, as such, compatible with both Article 6 and Article 8 of the ECHR. 272

V. COMPARING BRITISH AND AMERICAN SURVEILLANCE LAW

It is time to venture some comparative conclusions about the merits of the respective systems of authorization and oversight of interception of communications in the United Kingdom and the United States. To do so, it is instructive to look, first, at the structures, procedures, and actual operation of the two systems, and, second, at statistics on the per capita incidence of wiretapping in Britain, the United States, and other jurisdictions.

A. Structures, Procedures, and Operational Realities

In the United States, wiretap orders in criminal investigations are sought from a state or federal judge pursuant to procedures established by Title III. In operations aimed at acquiring foreign intelligence information, the government is required to seek interception orders from a judge of the FISA

272 Kennedy, App. No. 26839/05, Eur. Ct. H.R. paras.169–170. Despite receiving the approval of the ECtHR for their current surveillance regime, policy makers in the UK are on the verge of instituting major changes. In 2015, and in direct response to Edward Snowden’s 2013 revelations, three major reports were issued. First, the Intelligence and Security Committee issued a report advocating retention of the existing system of ministerial authorization for interception warrants. See INTELLIGENCE AND SECURITY COMMITTEE, PRIVACY AND SECURITY: A MODERN AND TRANSPARENT LEGAL FRAMEWORK, 2015, H.C., at 7, 73–76 (U.K.). That same year, David Anderson, the Independent Reviewer of Terrorism Legislation, also issued a report advocating the establishment of an Independent Surveillance and Intelligence Commission (ISIC). See DAVID ANDERSON, ISIC, REPORT OF THE INVESTIGATORY POWERS REVIEW: A QUESTION OF TRUST 6–8 (2015), available at https://www.gov.uk/government/publications/a-question-of-trust-report-of-the-investigatory-powers-review. Members of the Commission—termed “Judicial Commissioners”—would take over direct responsibility for approval of interception warrants in criminal cases and “national security [cases] of a domestic nature.” Id. at 274. In cases in which the Secretary of State certified that a warrant was required in the interests of “the defence and/or foreign policy of the UK,” a Judicial Commissioner would exercise judicial review—presumably rather lenient judicial review—of the Secretary of State’s certification. See id. at 270–75. Finally, the Royal United Services Institute for Defence and Security Studies (RUSI) also issued a report recommending a “composite approach” similar to that advocated by David Anderson. See RUSI, REPORT OF THE INDEPENDENT SURVEILLANCE REVIEW: A DEMOCRATIC LICENCE TO OPERATE 81–83, 97–100, 111–12 (2015), available at https://www.rusi.org/downloads/assets/ISR-Report-press.pdf. For a brief discussion of the response of the Cameron and May Governments and Parliament to the foregoing recommendations, as of October 2016, see infra notes 317–29 and accompanying text.
Court. In the United Kingdom, all requests for authority to engage in interception of communications within the country are directed to the Secretary of State for the Home Department. The Home Secretary is solely responsible for issuing interception warrants not only to the Security Service for intelligence-gathering purposes but also to the police for ordinary criminal investigations.

The interception regimes of both the United States and the United Kingdom therefore require operations-level executive branch law enforcement and counter-intelligence officials to seek prior approval from a third party for their decisions to resort to wiretapping. However, the United States has embraced a decentralized system of judicial pre-approval that owes its origins to perceived abuses of the warrant-granting power on the part of British secretaries of state in the eighteenth century. In contrast, the United Kingdom has chosen to vest power in the official whose conduct prompted the Americans to become leading proponents, in the latter half of the twentieth century, of the supposed virtues of judicial oversight of the use of electronic surveillance.

Which system does a better job of achieving the oft-repeated goal of striking a “proper balance” between the need to combat crime and protect national security, on the one hand, and the need to safeguard citizens’ privacy rights, on the other? The answer is not obvious. On the one hand, a centralized system of interception warrants would seem by definition to heighten the risk that government surveillance could be directed at political dissidents or could otherwise be used for improper or oppressive purposes. On the other hand, as the authors of the Birkett Report remarked, it is arguable that in a decentralized system in which “a number of magistrates or judges [have] the power to issue such warrants, the control of the use to which methods of interception can be put would be weaker than under the present system.”273 On this issue, it is only fair to say that we do not know, in the abstract and with certainty, which system is superior.

What can be said is that the decentralization of the American system, at least in federal cases, is easily exaggerated. Warrant requests are funneled through the Electronic Surveillance Unit of the Office of Enforcement Operations of the Criminal Division of the Department of Justice, after which they are presented to the Attorney General or a specially designated high-level Justice Department official for signature.274 In the case of the

---

273 BIRKETT REPORT, supra note 98, ¶ 86.
274 See supra note 25 and accompanying text.
FISA Court, applications are prepared and filed by the National Security Division of the Justice Department and require the approval of the Attorney General. In the United States, therefore, the DOJ is responsible for “quality control” of warrant applications, and, at least within individual presidential administrations, there is probably substantial consistency in the standards to which warrant applications are held prior to being forwarded to the chambers of individual federal judges. On its face, the process of preparing warrant requests for such judges bears a striking resemblance to the steps taken by the British Home Office in preparing warrant requests for eventual submission to the Secretary of State.

1. Operational Realities of the Warrant-Granting Process

What do we know about how state and federal judges in the United States and the Secretary of State in the United Kingdom actually exercise their warrant-granting power? The answer, it seems, is quite a lot but not nearly enough.

In both the United States and the United Kingdom, raw statistics on the ease of gaining approval for wiretapping are accessible and fairly straightforward. In the United States, between 1968 and the end of 2013, state and federal judges authorized some 55,386 interception warrants pursuant to Title III. In that same period, judges denied a total of thirty-nine warrant requests. In the FISA Court, between 1979 and 2011, judges approved a total of 32,087 government applications for authority to conduct electronic surveillance and/or physical searches for foreign intelligence purposes. In that period, a total of twelve applications were rejected.

275 See supra notes 46–47 and accompanying text.
276 Whether there is comparable consistency in the content and caliber of warrant applications submitted by state officials to state court judges—which constitute about two-thirds of Title III approvals—is another question. See infra notes 278–79, 297 and accompanying text.
277 See supra note 163 and accompanying text.
279 Id.
281 Id.
Turning to the United Kingdom, in the decade between 2001 and the end of 2010, the Home Secretary issued a total of 16,668 warrants for domestic interception of communications.\footnote{This figure is calculated from statistics published in the Interception of Communications Commissioner’s annual report for 2001 through 2010. Beginning in 2011, the Commissioners have reported only a total figure for “the Secretaries”—including not only the Home Secretary but also the Defence and Foreign Secretaries and the Scottish Ministers. Warrants issued by the Home Secretary authorize “domestic” wiretapping in the UK for both law enforcement and intelligence-gathering purposes and thus correspond most closely to the combined number of two categories of American warrants: (1) Title III warrants approved by state and federal judges and (2) FISA Court warrants issued for domestic surveillance. For purposes of comparative analysis, therefore, I will rely primarily on British and American figures reported for years prior to 2011. See Interception of Communications Commissioner, Annual Report, 2011–12, H.C. 496, at 29 (U.K.).} It is safe to assume that few requests are denied. However, little information is available on this question in the Annual Reports of the Interception of Communications Commissioner. In his Annual Report for 2010, for instance, the Commissioner noted only that “[t]he outright refusal of an application is rare,” but he provided no further details.\footnote{Interception of Communications Commissioner, Annual Report, 2010, H.C. 1239, ¶ 2.4 (U.K.).}

The bottom line is that in both the United States and the United Kingdom, the ratio of warrant denials to warrant approvals is miniscule. This does little more, however, than raise the perennial question of whether the low rate of denials is the product of hopelessly lenient standards for approving interception warrants or is instead a reflection of the self-restraint and professionalism of operations-level executive branch officials. Civil libertarians are quick to embrace the former explanation. Government officials are equally fond of the latter explanation. Arriving at a true assessment of whether a particular system of surveillance authorization and oversight exhibits a satisfactory level of rigor in balancing privacy against security and public order is not an easy task.

2. \textit{Ex Post Scrutiny of Authorized Wiretapping}

The situation is not significantly improved if we examine what we know about ex post scrutiny of the merits of granted warrants. With respect to FISA Court orders, post-surveillance notification of targets does not occur unless the government elects to prosecute the target for a criminal offense.\footnote{See supra note 48 and accompanying text.} As a result, most FISA surveillance begins and ends without anyone other
than the FISA Court and the government being aware of that fact. When prosecutions do occur, defendants are informed that the government intends to rely on FISA-derived evidence, and, in about 35–40 cases, they have sought disclosure. However, no defendant has ever succeeded in gaining access to any “applications or orders or other materials,” let alone in convincing a judge to order suppression of the resulting evidence.285

Title III includes a much more expansive post-surveillance notification requirement than FISA.286 Thus, there are numerous opportunities for defendants (and others) to challenge the merits of a Title III interception order. The problem here is the enormity of the data set. In the FISA context, Professor Patricia L. Bellia has highlighted the complete absence of successful challenges to the introduction of FISA-derived evidence.287 After doing so, she adds that “[a]lthough suppression is also quite rare in the Title III context, the sheer number of suppression motions under Title III makes tabulation and comparison impossible.”288

Focusing strictly on the United States, therefore, the absence of substantive information about the soundness of the warrant-granting decisions of FISA Court judges, combined with the unwieldy amount of information about the fate of Title III challenges, makes it difficult to compare the warrant-granting behavior of federal judges presiding over criminal cases to that of federal judges who serve on the FISA Court. In cases governed solely by Title III, the sheer quantity of relevant judicial decisions inhibits ready comparison of the behavior of federal judges to that of their state court counterparts.

It is equally difficult to reach objective comparative conclusions about the care or professionalism with which American judges and British secretaries of state execute their warrant-granting responsibilities. With respect to the response of British secretaries of state to warrant requests, this Article has already noted the Commissioner’s concession that “[t]he outright refusal of an application is rare.”289 However, no specific information on the ratio of grants to denials is publicly available, and thus the behavior of the Secretary of State and that of American judges cannot easily be compared, apart from noting that requests for warrants are very rarely denied in either jurisdiction.

285 See supra notes 49–54 and accompanying text.
286 See supra notes 26–27 and accompanying text.
287 Bellia, supra note 52, at 341.
288 Id. at n.182.
289 See supra note 283 and accompanying text.
As for ex post scrutiny of alleged unlawful interception in the United Kingdom, once the Home Secretary agrees to issue a warrant, challenges to its lawfulness are channeled exclusively to the Interception of Communications Tribunal (between 1986 and 2000) and the Investigatory Powers Tribunal (2000 to the present). There are gaps in our knowledge, but it does not appear that any allegation of unlawful telephone tapping submitted to the ICA between 1986 and 2000 was upheld.\textsuperscript{290} With the passage of RIPA 2000, the IPT assumed responsibility for hearing complaints about various types of surveillance, including, but not limited to, interception of communications. In 2005, the Tribunal upheld a complaint for the first time, and it has upheld a handful of other complaints since; however, none of the successful complaints alleged that the government was engaged in unlawful telephone tapping.\textsuperscript{291} Thus, it does not appear that any complaint of such tapping has ever been upheld.

3. Conclusion

Our ability to reach meaningful conclusions about the relative merits of the British and American systems of interception of communications is severely hampered by several features of the two systems. Analysis in both systems is handicapped by the enigmatic significance of the near-perfect record of executive officials in gaining approval for their warrant requests. In addition, both jurisdictions are notable for the secrecy that surrounds key components of their warrant-granting and warrant-reviewing processes. Finally, the sheer magnitude of the body of judicial and other decisions requiring scrutiny frustrates meaningful analysis. In the end, the only hope for shedding light on the operational merits of the two systems may be to devise an in-depth field study or a massive empirical study. In the meantime, we know that interception of communications in the United States requires a

\textsuperscript{290} \textit{Interception of Communications Commissioner, Annual Report, 1997} (H.C.), Cm 4001, at 5 (U.K.) (reporting none of the 568 complaints received by the tribunal had been upheld). \textit{Interception of Communications Commissioner, Annual Report, 1998} (H.C.), Cm 4364, at 6 (U.K.) (reporting none of the seventy-five further complaints received by the tribunal had been upheld).

\textsuperscript{291} See \textit{Operation-Cases Upheld}, Investigatory Powers Tribunal (June 29, 2014), http://www.ipt-uk.com/section.aspx?pageid=9. See also Anderson, supra note 272, ¶ 6.106 (the “profile of the IPT as a robust scrutiny mechanism was not assisted by the fact that out of the 1,673 complaints determined by the end of 2013, only 10 were upheld---five of them involving members of the same family, and none of them against the security and intelligence agencies”).
judicial warrant and interception in the United Kingdom requires an executive warrant and that warrant requests from executive branch officials in both jurisdictions are rarely denied. Beyond that, the available information is either overwhelming in scope, difficult to interpret, or unavailable.

B. The Incidence of Wiretapping

Another approach to comparing the British and American surveillance regimes to one another—and to regimes in operation in other countries—is to look at statistics on the per capita incidence of authorized governmental wiretapping. This method of drawing comparisons is not without weaknesses, because there will be national differences in the way in which wiretap statistics are compiled and other factors that could produce misleading conclusions. Nevertheless, it is instructive to examine what we know about the incidence of wiretapping in various jurisdictions as one way of assessing the relationship between citizens and their governments and the extent to which individual privacy is or is not adequately protected.

1. Wiretapping in the United States

In the United States, wiretap orders approved pursuant to Title III are reported annually in the Wiretap Report of the Director of the Administrative Office of the United States Courts, which includes statistics on orders issued by both state and federal judges. Basic information on the number of applications to the FISA Court for authority to conduct electronic surveillance for foreign intelligence purposes is reported annually in a letter from the Department of Justice to congressional leaders.

As noted above, a total of 55,386 Title III warrants were issued by state and federal judges between 1968 and 2013. Therefore, in the forty-six year history of Title III, state and federal judges have issued an average of about 1,204 warrants per year. Between 1979 and 2013, the FISA Court

294 See supra note 278 and accompanying text.
approved a total of 35,434 government applications for a FISA order.\textsuperscript{295} Thus, FISA Court orders have averaged roughly 1,012 per year.

Predictably, the number of Title III warrants has risen—from an average of 679 per year in the twelve years between 1970 and 1981 to an average of 1,933 in the twelve years between 2000 and 2011.\textsuperscript{296} Thus, the frequency of the issuance of such warrants has approximately tripled.\textsuperscript{297} Between 1980 and 1991, the FISA Court approved an average of 530 orders per year.\textsuperscript{298} In the recent twelve-year period between 2000 and 2011, the court averaged 1,666 approvals per year. Thus, FISA Court orders, like Title III warrants, have approximately tripled.\textsuperscript{299}

In the twelve-year period between 2000 and 2011, the combined average of Title III warrants and FISA Court orders issued every year—1,933 Title III warrants plus 1,666 FISA Court orders—is about 3,600. Assuming a U.S. population of 300 million people, state and federal courts and the FISA Court thus issue about 1.2 interception warrants/orders per 100,000 persons per year for the purpose of domestic collection of evidence of criminal activity and domestic collection of foreign intelligence information.

2. Wiretapping in the United Kingdom

In the decade between 2001 and 2010, the Home Secretary issued 16,668 warrants for domestic interception of communications for the purpose of combating serious crime and/or protecting national security.\textsuperscript{300} In recent years, therefore, the average number of warrants issued every year has been

\textsuperscript{295} See supra note 280 and accompanying text.
\textsuperscript{296} I have excluded 1968 and 1969 from this calculation, because Title III warrants increased rapidly (from 174 in 1968 to 596 in 1970) in the initial period of the operation of the legislation.
\textsuperscript{297} In both the recent twelve-year period and over the forty-six-year history of Title III, warrants issued by state judges have been approximately twice as numerous as warrants issued by federal judges.
\textsuperscript{298} I have excluded 1979 from this calculation, because the Court did not operate for the full year.
\textsuperscript{299} This may seem surprising, given the presumed impact of September 11 on the activity of the FISA Court. It becomes less surprising when account is taken of the fact that investigation of drug offenses is the dominant purpose of the issuance of Title III warrants and that such offenses have arguably increased at a faster pace than terrorist threats. In 2012, for instance, “87 percent of all applications for intercepts [cited] illegal drugs as the most serious offense under investigation.” Admin. Office of U.S. Courts, Wiretap Report 2012, available at http://www.uscourts.gov/Statistics/WiretapReports/wiretap-report-2012.aspx.
\textsuperscript{300} See supra note 282 and accompanying text.
about 1,666. Taking this figure at face value, and assuming a population of about 60 million people, the Secretary of State issues about 2.75 warrants per year per 100,000 persons. The incidence of the issuance of interception warrants thus appears to be a little over twice as great in the United Kingdom as in the United States.\footnote{One must be very cautious about drawing conclusions from a statistic such as this. To mention only one confounding factor, there is every reason to believe that the threat from indigenous terrorists is substantially greater in Britain than in the United States. For a discussion of the perils of relying on reported statistics to compare surveillance regimes in various jurisdictions, see Schwartz, supra note 11, at 1250–54; Schwartz, supra note 60, at 758–64.}

3. Wiretapping in Other Jurisdictions

To put these statistics in perspective, it is useful to examine what we know about the incidence of wiretapping in other jurisdictions. For this purpose, we can turn to recent ECtHR decisions on interception of communications in Bulgaria and Moldova.

a. Bulgaria

In 2007, the ECtHR examined the Convention-compatibility of Bulgaria’s Special Surveillance Means Act of 1997 (SSMA) and also examined the manner in which the law operated in practice.\footnote{Ass’n for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, App. No. 62540/00, 533 Eur. Ct. H.R. (2007), available at http://hudoc.echr.coe.int/eng?i=001-81323. Bulgaria ratified the European Convention on Human Rights, and accepted the compulsory jurisdiction of the European Court of Human Rights, in 1992.} The SSMA authorized various police and internal security agencies to engage in wiretapping, and judges were given responsibility for issuing warrants. After the issuance of a warrant, however, control of the surveillance process reverted to the Minister of Internal Affairs.\footnote{ld. paras. 15, 27.} In addition, according to the court, “under Bulgarian law the persons subjected to secret surveillance are not notified of this fact at any point in time and under any circumstances.”\footnote{ld. para. 90.}

The ECtHR held that the SSMA, even as written, failed to satisfy the requirement of Article 8(2) of the ECHR that any interference with rights protected by Article 8(1) must be “in accordance with the law.”\footnote{ld. paras. 93.} After reviewing its precedents on “foreseeability” and “compatibility with the rule...
of law,”306 the court noted that “while in certain respects Bulgarian law fully comports with the above requirements, in other respects it falls short.”307 In particular, the court found fault with the fact that control of surveillance reverted to the Ministry of Internal Affairs following its initial authorization by a judge.308

The ECtHR also reviewed statistics on the number of wiretap warrants issued by judges in the first place. It noted that a report issued by the Bulgarian Supreme Cassation Prosecutor’s Office found that in a two-year period from 1999 through 2000, “more than 10,000 warrants were issued, [and] that number does not even include the tapping of mobile phones.”309 Taken at face value, and based on a population of approximately 7.3 million, the incidence of wiretapping in Bulgaria therefore works out to more than seventy orders per 100,000 persons. If true, this means that the per capita use of wiretapping in Bulgaria is roughly twenty-five times greater than in the United Kingdom and more than fifty-five times greater than in the United States. The court’s conclusion was that compared to other countries, “the system of secret surveillance in Bulgaria is, to say the least, overused.”310

b. Moldova

Moldova ratified the ECHR in 1997. In 2002, members of a non-governmental organization called “Lawyers for Human Rights” filed an application with the ECtHR alleging that Moldovan law governing telephone tapping violated Article 8 of the ECHR. Their challenge to Moldovan law was resolved by the ECtHR in 2009.311

In Iordachi, the court examined Moldova’s Operational Investigative Activities Act. The law prescribed that investigative measures “which infringe lawful rights,” including the secrecy of telephone conversations, “shall be permitted [only] with the authorisation of the investigating judge.”312 A separate statute, the Code of Criminal Procedure, required that

306 Id. paras. 74–77. See also supra notes 146–55 and accompanying text.
308 Id. para. 85.
309 Id. para. 92.
310 Id.
312 Id. para. 14.
“after the end of an authorized interception [the] judge shall inform in writing the persons whose conversations were intercepted.”

In their application to the ECtHR, the lawyers challenging the Moldovan regime of interception of communications told the court that in their experience “no investigating judge had ever complied” with the obligation to provide post-surveillance notification to persons whose telephone calls had been intercepted. In addition, they provided the court with a letter from the Head of the President’s Office of the Supreme Court of Justice indicating that investigating judges had granted an average of 2,274 interception authorizations per year in 2005–2007. In a country of 3.5 million, this translates into roughly 65 authorizations per 100,000 inhabitants, and it prompted the court to remark, as it had in AEIHR and Ekimdzhiev, that the “figures show that the system of secret surveillance in Moldova is, to say the least, overused.”

4. Conclusion

The ECtHR’s decisions in AEIHR and Ekimdzhiev and in Iordachi are a reminder that historical experience and political culture can play a major role in the operation of a country’s surveillance regime, however much its statutory components may resemble an American-style system requiring judicial pre-approval and other safeguards against abuse of citizens’ privacy rights. On its face, the Bulgarian system included judicial pre-approval of wiretap decisions. The Moldovan system included judicial pre-approval of wiretap decisions and post-surveillance notification by an investigating judge of the targets of covert surveillance. In practice, however, both systems exhibited serious weaknesses, and it was apparent to the ECtHR that neither system had yet achieved much success in escaping the baleful effects of its totalitarian past.

VI. CONCLUSION

The American system of authorized governmental interception of communications—consisting not only of judicial pre-approval of executive branch wiretapping decisions but also of innumerable individual decisions by

---

313 Id. para. 17.
314 Id. para. 22.
315 Id. para. 13.
316 Id. para. 52.
both state and federal judges—stands in marked contrast to the concentration
of warrant-granting power in the hands of a single executive official in the
United Kingdom. The American system of judicial pre-approval is self-
evidently more attractive to civil libertarians. In addition, the British system
exhibits a higher level of secrecy than the American system (although the
differences are not substantial in the case of covert surveillance aimed at
gathering intelligence and countering threats to national security). For this
reason as well, the American system is preferred by groups and individuals
who put a high premium on protection of privacy.

Looking at the systems as a whole, however, it is surprisingly difficult to
conclude that one is significantly more successful than the other at striking
the proper balance between the needs of the state and the rights of the
individual. While interception of communications in the United Kingdom is
firmly controlled by the government and thoroughly shrouded in secrecy,
executive branch officials operate within an elaborate system of judicial, or
at least “quasi-judicial,” safeguards. The roles that the Commissioner and
the IPT play in overseeing interception of communications contrast rather
sharply with role of judges in the more widely used American system. How-
ever, both the Commissioner and the members of the IPT boast
impressive legal and judicial credentials. Moreover, the statutory role they
play, in conjunction with the Secretary of State’s personal responsibility for
issuing interception warrants, has persuaded the ECtHR that there exist in the
British system “adequate and effective guarantees against abuse.” Most
observers agree that permitting government to engage in interception of
communication is a “necessary evil.” That being the case, Britain and the
United States have probably done as sound a job as any modern jurisdiction
of crafting effective arrangements for simultaneously protecting the privacy
rights of individuals at whom such interception is directed.

Postscript

On November 4, 2015, the British Home Secretary, Teresa May,
published the Cameron Government’s “Draft Investigatory Powers Bill.”317
The Government accepted some, but not all, of the recommendations of three
reports published the previous summer.318 In particular, the Government
proposed to establish a “double-lock” system whereby interception warrants
for both law enforcement and national security purposes would continue to

317 SECRETARY OF STATE FOR THE HOME DEPARTMENT, DRAFT INVESTIGATORY POWERS BILL,
2015, Cm. 9152 (U.K.), available at http://www.gov.uk/government/publications/draft-investi-
gatory-powers-bill.
318 See supra note 272 and accompanying text.
be issued by the Secretary of State but could not come into force until approved by a Judicial Commissioner, who would be a serving or former High Court judge. In addition, the Investigatory Powers Tribunal would be retained, but there would be a right of appeal to the Court of Appeal on a point of law from a determination of the tribunal. However, leave to appeal would need to be granted by the IPT, or, if refused, by the Court of Appeal. In addition, leave to appeal could not be granted by either the IPT or the Court of Appeal unless it considers that “the appeal would raise an important point of principle or practice [or] there is another compelling reason for granting leave.”

Following publication of the Draft Bill, Parliament appointed an ad hoc Joint Committee on the Draft Investigatory Powers Bill, which held hearings between November 30, 2015, and January 13, 2016. On February 11, 2016, the Joint Committee published its report. The Committee noted that “[t]he draft Bill introduces an extra layer of judicial authorisation for powers that have previously been subject to ministerial authorisation only,” and it concluded that it was “satisfied that a case has been made for having a ‘double-lock’ authorisation for targeted interception.”

The Committee raised questions, however, about other aspects of the draft Bill, including the role assigned to Judicial Commissioners in conducting general oversight of the warrant-granting system (as distinct from their role in approving the Secretary of State’s decisions to issue individual warrants), the limited scope of the right to appeal from decisions of the Investigatory Powers Tribunal, and the Government’s decision to perpetuate a high level of secrecy in connection with deliberations of the Tribunal. The Home Office considered the Committee’s report and other responses to its draft Bill and submitted revised legislation to Parliament on

320 Id.
321 Id. ¶¶ 175–176.
322 Id. ¶ 176.
323 For video of the joint committee’s hearings as well as transcripts of oral testimony and written evidence it received, see Joint Committee on the Draft Investigatory Powers Bill, UK Parliament, http://www.parliament.uk/draft-investigatory-powers.
325 Id. ¶¶ 411–422.
326 Id. ¶¶ 565–575, 609–612.
327 Id. ¶¶ 650–646.
328 Id. ¶¶ 657–663.
March 1, 2016. By the beginning of October 2016, the Bill—to be known as the Investigatory Powers Act 2016—had completed most of the stages of parliamentary scrutiny and was expected to be enacted into law by the end of the year.329

329 A running account of the progress of Parliament’s deliberations is published at http://services.parliament.uk/bills/2015-16/investigatorypowers.html.