Buffalo Public Interest Law Journal

Volume 29 Article 1

9-1-2010

"Ordinary Citizens" or a License to Kill? The Turn to Law in Regulating Britain's Intelligence Services

Simon Chesterman
New York University School of Law

"ORDINARY CITIZENS" OR A LICENSE TO KILL? THE TURN TO LAW IN REGULATING BRITAIN'S INTELLIGENCE SERVICES

SIMON CHESTERMAN†

† Simon Chesterman (D.Phil., Oxford; LL.B. & B.A., Melbourne) is Vice Dean and Professor of Law at the National University of Singapore and Global Professor and Director of the New York University School of Law Singapore Programme. This Article draws heavily upon material discussed at greater length in ONE NATION UNDER SURVEILLANCE: A NEW SOCIAL CONTRACT TO DEFEND FREEDOM WITHOUT SACRIFICING LIBERTY (Oxford University Press, 2011).

> The members of the Service are, in the eye of the law, ordinary citizens with no powers greater than anyone else. They have no special powers of arrest such as the police have. No special powers of search are given to them. They cannot enter premises without the consent of the householder, even though they may suspect a spy is there.... They have, in short, no executive powers. They have managed very well without them. We would rather have it so, than have anything in the nature of a "secret police."
> *Lord Denning*[1]

In the mid-1970s, James Malone was an antique dealer living in Dorking, a historic market town in Surrey, England.[2] He began receiving mail that was opened and resealed with identical tape and suspected that his phone was tapped. It transpired that he was the target of a police investigation and in 1977 he was charged with receiving stolen goods.[3] Two trials ended with hung juries and a third attempt at prosecution was abandoned. However, during the first trial, a police officer under cross-examination read from a notebook what appeared to be extracts of telephone conversations.[4] This departure from police practice at the time—which was never to reveal the use of wiretapping—led to a countersuit by Malone challenging the lawfulness of the intercept. That case was dismissed as the judge concluded that there was no law prohibiting such wiretapping in England, but he added that the potential for abuse made this a subject that "cries out for legislation."[5]

Malone pursued his complaint to the European Court of Human Rights, which allows an individual right of petition to

---

[1] Lord Denning, Report on the Profumo Affair (HMSO, London, Cmnd 2152, 1963), para 273.
[2] Malone v. Metropolitan Police Comm'r [1979] Ch 344, 349.
[3] *Id.*
[4] *Id.*
[5] *Id.* at 380.

challenge violations of the European Convention on Human Rights. The Convention includes a right to privacy, which is not to be interfered with except "in accordance with the law" and as necessary in a democratic society in pursuit of national security, public safety, for the prevention of crime, and other defined aims.[6] What became clear was that the British guidelines for granting wiretaps were vague to the point of obscurity. The Court held that the law did not indicate with reasonable clarity the extent of discretion conferred on the public authorities,[7] and 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."[8]

Malone won his case and a measure of damages, but the more lasting result was the passage of the Interception of Communications Act 1985.[9] This was the first in a series of statutes that brought the British intelligence services and their powers onto a legislative footing. For the better part of four decades, the Security Service (better known as MI5) operated on the basis of a six paragraph administrative directive until legislation was passed in 1989. The British government only officially acknowledged even the existence of the Secret Intelligence Service (known as MI6) in 1992—well after the release of the sixteenth James Bond film popularizing the exploits of its most famous fictional agent.

Here the focus will be the impact that the formalization of the intelligence services and their powers has had in Britain. As Lord Denning indicates, Britain long adopted the legal fiction—manifestly false in practice if not in theory—that the representatives of its intelligence services were merely "ordinary

---

[6] [European] Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, 213 UNTS 222, art 8.

[7] Malone v. United Kingdom, 7 EHRR 14 (1985), para 79.

[8] *Id.* at para 68.

[9] IAN LEIGH & LAURENCE LUSTGARTEN, IN FROM THE COLD: NATIONAL SECURITY AND PARLIAMENTARY DEMOCRACY 69 (1994).

citizens."[10] In fact, the agents of these services exercised considerable power and the move towards establishing a legal foundation for those powers and appropriate checks and balances in the past two decades are, as the European Court held, demanded by the rule of law.[11] At the same time, however, Britain demonstrates some of the problems attendant to establishing such a legal regime. These include the question of how the mandate of intelligence services should be defined, as well as the possibility that powers granted by law may be exercised by a far wider range of actors than when a key check was the need to keep those powers and actors secret. Finally, Britain is of interest in showing the limitations of law in regulating socially-pervasive technologies, such as the closed-circuit television (CCTV) cameras that are ubiquitous in London and other cities large and small. The belated effort to regulate CCTV suggests lessons for other new technologies such as biometric identification and DNA databases.

I. "ORDINARY CITIZENS"

The *Malone* case highlighted a key difference between the U.S. and British approaches to intelligence. The United States, somewhat unusually for the English-speaking world, put its intelligence services on a statutory basis very soon after the Second World War. This was consistent with the strict separation of executive and legislative powers under the U.S. Constitution, which vest in the distinct institutions of the President and Congress. In Britain and the rest of the Commonwealth, by contrast, the intelligence services traced their origins and powers—like all military matters—to the royal prerogative.[12] The protections against abuse of those powers were similarly distinct: in the United States the written Constitution and its Bill of Rights could be used to strike down legislation; in Britain the lack of a written constitution and the recognition of few formal rights meant

[10] Lord Denning, *supra* note 1, at para 273.
[11] *Malone,* 7 EHRR at paras 67-68.
[12] LEIGH & LUSTGARTEN, *supra* note 9, at 374.

that liberties (such as privacy) were traditionally protected only through the *absence* of legislation.[13]

The military origins of the Security Service and the Secret Intelligence Service live on in their colloquial names MI5 and MI6: Military Intelligence, Sections 5 and 6—administrative divisions dating back to the First World War, but not in active use since the 1920s.[14] (Section 1, dealing with codes and ciphers, ultimately became what is now Government Communications Headquarters, or GCHQ.) MI5 effectively reported to the Prime Minister until 1952, when responsibility was transferred to the Home Secretary. The shift was intended to bring MI5 under some measure of ministerial responsibility as the previous arrangement had allowed its Director-General virtual autonomy.[15] Sir David Maxwell-Fyfe, the Home Secretary at the time, wrote up a six paragraph directive addressed to the Director-General that provided the contours of the governance, mandate, and powers of MI5 for the next four decades.[16]

The governance structure was that the Director-General would be "personally" responsible to the Home Secretary, though MI5 itself remained part of the Defense Forces.[17] The directive also maintained the "well-established convention" that ministers would not concern themselves with the detailed information obtained by the Security Service in particular cases, "but are furnished with such information only as may be necessary for the

---

[13] Specific statutes did protect certain rights, such as the Data Protection Act 1984 (UK). Case law had also provided limited protections to home life. *See generally* Basil Markesinis et al., *Concerns and Ideas About the Developing English Law of Privacy (and How Knowledge of Foreign Law Might Be of Help)*, 52 AM. J. COMP. L. 133 (2004) (discussing the effect the European Convention on Human Rights is having on United Kingdom's domestic laws, specifically an individual's right to privacy).

[14] LEIGH & LUSTGARTEN, *supra* note 9, at 374.

[15] *Id.* at 375.

[16] *Id.*

[17] *Id.*

determination of any issue on which guidance is sought."[18] The mandate was framed broadly as "the Defence of the Realm as a whole" from internal and external espionage and sabotage, but also against the actions of persons and organizations "which may be judged to be subversive to the State."[19] At the same time, the directive emphasized the need to keep MI5 free of any political bias or influence, and that no investigations should be undertaken on behalf of a government department unless an important public interest bearing on the "Defence of the Realm" was at stake.[20] The agency's powers were not defined, but a further caveat enjoined the Director-General to "take special care to see that the work of the Security Service is strictly limited to what is necessary for the purposes of their task."[21]

In addition to the breadth of the discretion it conferred, the Maxwell-Fyfe Directive lacked any legal mechanisms to deal with complaints about abuses and violations of rights. It was also a mere administrative directive that could be changed without reference to Parliament, establishing no formal limits or controls.[22] Following the *Malone* decision—which dealt with the surveillance powers of the police rather than the intelligence services as such—it was clear that these deficiencies would be open to challenge before the European Courts.

II. THE RULE OF LAW

In practice, of course, members of the intelligence services exercised powers far beyond those of "ordinary citizens". As Peter Wright, a former Assistant Director of MI5, put it in his scandalous

---

[18] Maxwell-Fyfe Directive (issued by the UK Home Secretary, Sir David Maxwell-Fyfe, to the Director-General MI5, 1952) ("Maxwell-Fyfe Directive"), *reprinted in id.*at 517.

[19] *Id.*

[20] *Id.*

[21] *Id.*

[22] Ian Leigh, *Accountability of Security and Intelligence in the United Kingdom*, *in* WHO'S WATCHING THE SPIES: ESTABLISHING INTELLIGENCE SERVICE ACCOUNTABILITY 79, 79-80 (H. Born, Loch K. Johnson & Ian Leigh eds., 2005).

and self-aggrandizing memoir *Spycatcher*: "we, bugged and burgled our way across London at the State's behest, while pompous bowler-hatted civil servants in Whitehall pretended to look the other way."[23] Ironically, the use of telephone intercepts appears to have been subject to more thorough controls than other activities, though it was wiretapping in the *Malone* case that provided the impetus for change.[24]

Scandal is frequently the driving force for change in the legal regime governing intelligence. Britain is relatively unusual in that the most important change in the century since its modern intelligence services were established appears to have been inspired by the desire to *avoid* legal action. There had been criticism since the 1960s of the uncertain legal basis on which the intelligence services acted and the absence of protections against abuse.[25] Moves by former colonies such as Australia, New Zealand, and Canada to put their services on a legislative footing also influenced debate in Britain.[26] Other factors included the unwanted attention GCHQ had received because of a labor dispute in the mid-1980s,[27] and the futile efforts to suppress the publication of *Spycatcher*—which, predictably, boosted sales and undermined the British government's credibility.[28] Nevertheless, it appears to have been the threat of further human rights challenges in the European system that led to the surprise passage of the

---

[23] PETER WRIGHT, SPYCATCHER: THE CANDID AUTOBIOGRAPHY OF A SENIOR INTELLIGENCE OFFICER 54 (1987).

[24] *Id.* at 46. *See generally* CHRISTOPHER M. ANDREW, DEFEND THE REALM: THE AUTHORISED HISTORY OF MI5 (2009) (revealing the role of the Security Service in twentieth-century Britain).

[25] *See, e.g.*, ANDREW, *supra* note 24, at 756 (noting that the lack of British laws regarding privacy and telephone tapping led to the 1985 Interception of Communications Act).

[26] Ian Leigh & Laurence Lustgarten, *The Security Services Act 1989*, 52 MOD. L. REV. 801, 802 (1989).

[27] Council of Civil Service Unions v. Minister for the Civil Service [1985] AC 374 (known more commonly as the GCHQ Case).

[28] ANDREW, *supra* note 24, at 766; Leigh, *supra* note 22, at 80.

Security Service Act 1989 and, five years later, the Intelligence Services Act 1994.[29]

Though the *Malone* case did not directly involve the intelligence services, it set the benchmark for the exercise of surveillance powers and the need for them to be grounded in law.[30] In fact the interception of telecommunications, which had historically been assumed to be consistent with the common law (which recognized no right to privacy), had already been the subject of legislation. Prior to 1969, the Post Office was a part of the government and the Postmaster General was an officer of state. As a matter of policy, it was the practice at least from 1937 only to allow intercepts on the authority of the Home Secretary; any dispute between the Home Secretary and the Postmaster General was, presumably, resolved as a political matter within the cabinet.[31] In 1969, however, the Post Office was established as a public authority, no longer under ministerial control.[32] Language was included in the Post Office Act to preserve the same powers of interception, but framed in delightfully circumlocutory language:

> A requirement to do what is necessary to inform designated persons holding office under the Crown concerning matters and things transmitted or in course of transmission by means of postal or telecommunication services provided by the Post Office may be laid on the Post Office for the like purposes and in the like manner as, at the passing of this Act, a requirement may be laid on the Post-master General to do what is necessary to inform such persons concerning matters and things trans-mitted or in course of transmission by means of such services provided by him.[33]

---

[29] Leigh, *supra* note 22, at 80.
[30] Malone v. Metropolitan Police Comm'r [1979] Ch 344, 369-70.
[31] *Id.*
[32] Post Office Act 1969 (UK), s 6.
[33] *Id.* at s 80.

The effect was that the Home Secretary could continue to authorize wiretaps, but the indirection and vagueness with which this power was to be exercised is evident.

The need for any interference with the right to privacy to be "in accordance with the law" is understood under the European Convention as embracing two requirements. First, the law must be accessible: a citizen must be able to know the legal rules applicable to a given case. Secondly, those rules must be formulated with sufficient precision to enable him or her to foresee the consequences that any given action may entail.[34] The Court in *Malone* accepted that it was not appropriate to require that individuals should be able to foresee when the authorities were likely to intercept their own communications, but held that the law must nevertheless be sufficiently clear to give them an indication of when the authorities were empowered to resort to such secret and potentially abusive powers.[35]

In the case of interception of telecommunications, the legislation passed after the *Malone* decision made it a criminal offence to intercept post or telecommunications without a warrant issued by the Home Secretary and established a tribunal to hear complaints if unlawful interception was suspected.[36] The Act also prohibited the introduction of evidence of wiretapping in legal proceedings—presumably to avoid the type of mistake that had led to James Malone's troublesome lawsuit in the first place.[37] The legislation covering MI5 and MI6 was significantly broader, establishing their authority in legislation and under ministerial control, setting out their mandate and powers, and taking the first steps towards an accountability framework that included remedies for abuse of those powers. Though there was some criticism of the approach taken, the legislation succeeded in placating the European Convention organs, which dropped two pending cases

---

[34] Sunday Times v. United Kingdom [1979] 2 EHRR 245, para 49.
[35] Malone v. United Kingdom [1985] 7 EHRR 14, para 68.
[36] Interception of Communications Act 1985 (UK), ss 1 & 2.
[37] *Id.* at s 9.

concerning MI5 shortly after the Security Service Act came into force.[38]

A. Authority and Governance

The Security Service Act 1989 essentially preserved the constitutional framework of the Maxwell-Fyfe Directive: MI5 continued to operate under a Director-General who reported to the Home Secretary and, as necessary, to the Prime Minister.[39] It remained, therefore, under ministerial rather than parliamentary control. The budget for the agencies continued to be adopted in a "secret vote" as part of a global figure without breakdown or explanation of the details; ministers continued the convention of refusing to answer questions in parliament that concerned the agencies or touched on national security.[40]

This changed somewhat when the Intelligence Services Act 1994 was passed. As with its counterpart, MI6 was to continue operations broadly on the same basis as it had been, operating under a Chief—traditionally known as "C"—who reported to the Foreign Secretary and, as necessary, to the Prime Minister.[41] Similarly, GCHQ continued under a Director who also reported to the Foreign Secretary.[42] The Act provided for the creation of a new parliamentary committee (the Intelligence and Security

---

[38] Hewitt & Harman v. United Kingdom (Committee of Ministers, Dec. 13, 1990) Resolution DH (90) 36 (1990). *But see* P.G. & J.H. v. United Kingdom (European Court of Human Rights, Application no 44787/98, Sept. 25, 2001) (2001), paras 34-38. (Holding that the planting of a listening device in the suspect's flat violated Article 8 of the European Convention of Human Rights which guarantees a "right to respect for [] private life." *Id.* at para 37. The planting of the listening device did not conform to the "in accordance with the law" requirement of Article 8 because, as the British Government conceded, "at the time of the events there existed no statutory system to regulate the use of covert listening devices." *Id.*

[39] Security Service Act 1989 (UK), ("SSA 1989") ss 1-2.; *see also* Maxwell-Fyfe Directive, *supra* note 18, at 517.

[40] LEIGH & LUSTGARTEN, *supra* note 9, at 441-42, 447-50.

[41] Intelligence Services Act 1994 (UK) ("ISA 1994"), s 2.

[42] *Id.* at s 4.

Committee), which would examine the budget, administration, and policies of all three services.[43]

Such arrangements are broadly consistent with the situation in other Commonwealth countries, where heads of agencies report to the various ministers or equivalent. The directors of their US counterparts enjoy considerably more independence: they are appointed by the President and subject to confirmation of the Senate. Appointments therefore tend to be more politically driven. In the case of the FBI, Congress imposed a ten year term limit through legislation passed towards the end of J Edgar Hoover's half century at the helm.

B. Mandate

Both statutes sought to articulate the mandates of the agencies.[44] Eschewing the language of defense of the realm, the Security Service Act provided that the functions of MI5 are, first, "the protection of national security", in particular against threats from espionage, terrorism, sabotage, the activities of agents of foreign powers, and actions intended to overthrow or undermine parliamentary democracy.[45] In addition, MI5 is tasked with safeguarding the country's "economic well-being" against threats posed by "the actions or intentions" of persons outside the country.[46] The Intelligence Services Act 1994 was even more general, providing that the powers of MI6 and GCHQ are exercisable "only": (a) in the interests of national security, with particular reference to the defense and foreign policies of the government; (b) in the interests of the country's economic well-

---

[43] *Id.* at s 38.
[44] *Id.* at ss 1 (1)(a)-(b); SSA 1989, *supra* note 39, at s 1(2).
[45] SSA 1989, *supra* note 39, at s 1(2).
[46] *Id.* at s 1(3).

being; or (c) in support of the prevention or detection of serious crime.[47]

A mandate serves at least two important purposes for an intelligence agency. First, and most obviously, it sets boundaries on the information that the agency may collect and the people or activities it may target.[48] Given the history of many intelligence services and their tendency to show an excessive interest in domestic political protest and dissent, it is appropriate to put in place checks against activities that might lead to abuse or stifle political discourse.[49] These boundaries may or may not be subject to external enforcement, but can be important factors shaping the behavior of the officials in question.[50] As Leigh and Lustgarten concluded in their 1994 study of the security services of Britain, Canada, and Australia: "security officials are bureaucrats."[51] Though it would be unwise to rely on bureaucratic structures entirely, a clear and limited mandate shapes the internal rules and procedures of the bureaucracy; it influences the organizational culture and thus serves as a potent force for compliance.[52] Secondly, however, a mandate can provide a degree of protection for the agency itself.[53] There are obvious temptations for politicians to use the considerable powers of the intelligence services to political ends.[54] A well-crafted mandate can provide some insulation from these pressures.

In both areas, the British legislation represented a departure from best practice. On the establishment of boundaries, it is noteworthy that the British legislation governing MI5 offers an inclusive list of what is meant by the broad term "national security", whereas the comparable Australian and Canadian

---

[47] ISA 1994, *supra* note 41, at s 1(2). GCHQ's mandate uses almost identical language but its ability to act in the interests of Britain's economic well-being is limited to the actions or intentions of persons outside the country. *Id.* s 3(2).
[48] LEIGH & LUSTGARTEN, *supra* note 9, at 410-11.
[49] *Id.* at 411.
[50] *Id.*
[51] *Id.*
[52] *Id.*
[53] *Id.*
[54] *Id.*

statutes provide exhaustive definitions of "security." The Australian Security Intelligence Organization (ASIO) had previously operated on the basis of a "Charter" issued by the Prime Minister with many similarities to the Maxwell-Fyfe Directive before legislation was first adopted in 1956.[55] This and subsequent statutes defined security as including, among other things, protection against "subversion"—a notoriously elastic term that plausibly covers a range of legitimate political activities.[56] A Royal Commission later recommended that it be abandoned in favor of more specific reference to "politically motivated violence."[57] The legislation was also amended to provide that the powers granted to ASIO should not limit the right of persons to engage in "lawful advocacy, protest, or dissent" and that the exercise of these rights should not, in themselves, be regarded as falling within the mandate of the agency.[58] The latter amendment tracked language in a Canadian law passed two years earlier, which prevents the Canadian Security Intelligence Service (CSIS) from investigating lawful advocacy, protest, or dissent unless carried on in conjunction with one of the listed threats, which pointedly excluded subversion.[59]

On the insulation from political interference, the Maxwell-Fyfe Directive, for all its other deficiencies, may have been clearer

---

[55] Charter of the Australian Security Intelligence Organization (A Directive from the Prime Minister to the Director-General of Security) (Office of the Prime Minister, Canberra, 1950); Australian Security Intelligence Organization Act 1956 (Australia) ("ASIO 1956").

[56] *Id.* at s 4.

[57] Australian Security Intelligence Organization Amendment Act 1986 (Australia), st 3, 9; *see also* Royal Commission on Australia's Security and Intelligence Agencies, Report on the Australian Security Intelligence Organisation (AGPS, Canberra, 1984).

[58] Greg Carne, *Thawing the Big Chill: Reform, Rhetoric, and Regression in the Security Intelligence Mandate*, (1996) 22 MONASH U.L. REV. 379, 415, 428 (1996); JENNY HOCKING, TERROR LAWS: ASIO, COUNTER-TERRORISM AND THE THREAT TO DEMOCRACY 34-38 (2004).

[59] Canadian Security Intelligence Service Act 1984 (Canada) ("CSIS 1984"), s 2.

in its provision authorizing, or perhaps requiring, non-compliance with a request unless the Director-General was satisfied that an important public interest bearing on the Defense of the Realm was at stake.[60] It also required the Director-General to ensure that MI5 was kept absolutely free from any "political bias or influence," whereas the 1989 legislation confined this prohibition to "actions 'to further the interests of any political party.'"[61] Australia's legislation went further in providing that the Director-General of ASIO cannot be overridden by the Minister concerning the nature of advice given by the agency; on the collection and sharing of intelligence on a particular individual the Director-General can be overridden, but written instructions to that effect must be copied to the Inspector-General of Intelligence and Security and the Prime Minister.[62] Interestingly, Canada considered and rejected similar language because it reduced the direct political responsibility of the Minister.[63] Instead the CSIS Act provides that the head of the agency operates under the "direction of the Minister."[64]

The question of whether intelligence services need to be protected from undue influence depends, then, on whether that concern ranks higher than the danger that the service itself will act inappropriately, or that the political leadership will use that insulation to ensure the deniability of controversial activities.

C. Powers

Lord Denning's comment that the members of the Security Service were "ordinary citizens" was, at least technically, true. Before 1989, they enjoyed no special legal powers and their transgressions of the laws applicable to other "ordinary citizens" were either not detected by the police or not prosecuted through

---

[60] LEIGH & LUSTGARTEN, *supra* note 9, at 375.

[61] *Id.* at 378 (internal citation omitted) ; SSA 1989, *supra* note 39, at s 2(2)(b); ISA 1994, *supra* note 41, at s 2(2)(b).

[62] ASIO 1956, *supra* note 55, at s 8.

[63] Philip Rosen, The Canadian Security Intelligence Service (Library of Parliament, Research Branch, Ottawa, 84-27E, Jan. 24, 2000), at 8, *available at* http://www.parl.gc.ca/information/library/PRBpubs/8427-e.htm.

[64] CSIS 1984, *supra* note 59, at s 6(1).

the use of discretion.[65] The extent of those transgressions was, presumably, constrained by the injunction in the Maxwell-Fyfe Directive that the Service's work should be "strictly limited to what is necessary."[66]

The Security Service Act 1989 replaced this—or, more realistically, supplemented it—with a system whereby the Home Secretary may issue a warrant authorizing "entry on or interference with property."[67] Such a warrant confers immunity from criminal or civil liability for the action concerned.[68] The provision bears similarities to its Australian and Canadian counterparts but is somewhat broader. The comparable Australian provision is more specific about the purposes for which warrants may be authorized and the types of information that may be collected; warrants are also limited to 90 days rather than six months under the British provision.[69] The Canadian legislation is also more detailed and requires that warrants be issued by a Federal Court judge; at the same time it extends the duration of warrants to one year except for those enabling the investigation of the most general category of threat to the security of Canada, in which case the maximum duration is 60 days.[70]

The powers of foreign intelligence services tend to be considerably broader. As a general rule, actions in a foreign country are not subject to liability in one's own country.[71] The Intelligence Services Act went further in providing that the Foreign Secretary can authorize action outside of Britain that would otherwise subject a person to criminal or civil liability.[72] The Act is unclear as to what may be authorized, but among other things it

---

[65] Leigh & Lustgarten, *supra* note 26, at 822.
[66] Maxwell-Fyfe Directive, *supra* note 18, at 517.
[67] SSA 1989, *supra* note 39, at s 3(1).
[68] *Id.* at s 3.
[69] ASIO 1956, *supra* note 55, at s 25.
[70] CSIS 1984, *supra* note 59, at ss 21-23.
[71] *See* ISA 1994, *supra* note 41, at s 7.
[72] *Id.* at ss 7(1)-(2).

requires the Foreign Secretary to be satisfied that the action is necessary for the proper discharge of a function of MI6 and that the nature and likely consequences will be "reasonable."[73] With only slight exaggeration, this might be thought of as the statutory basis for James Bond's "license to kill"—though it requires renewal every six months.[74] The Australian Intelligence Services Act offers still broader protection to staff and agents of the Australian intelligence agencies from civil or criminal liability for any act outside the country if it was done "in the proper performance of a function of the agency."[75] This is limited by the requirement for ministerial authorization of collection activities involving an Australian person, but such authorizations are not required for other activities abroad.[76]

D. Remedies

Before the passage of legislation in the 1980s, essentially no remedies were available to citizens alleging abuse of powers by the intelligence services. In the first place, the absence of a right to privacy meant that much conduct was not, in fact, unlawful. Though the law did require a minimum degree of suspicion before a person or property could be seized, this did not apply to other conduct to gather information.[77] In any event, there was little judicial willingness to investigate wrongdoing in the absence of significant public outcry.[78]

With respect to MI5, the 1989 legislation established a Security Service Commissioner to review the exercise of the powers granted to the Service and a Tribunal to investigate complaints.[79] The Security Service Tribunal was empowered to investigate whether a person had been the subject of "inquiries" and, if so, whether the Service had reasonable grounds for

---

[73] *Id.* at s 7(3).
[74] *Id.* at s 7.
[75] Intelligence Services Act 2001 (Australia) ("ISA 2001"), s 14(1).
[76] *Id.* at s 8(1).
[77] Leigh & Lustgarten, *supra* note 26, at 829.
[78] *Id.* at 828-29.
[79] SSA 1989, *supra* note 39, at s 5(1).

instigating them.[80] If the Tribunal concluded that there were no such reasonable grounds, it could order that inquiries be terminated, records destroyed, and compensation paid[81]—though the complainant would merely get a notification as to whether or not a determination had been made in his or her favor.[82] No reasons would be given, though a report would be made to the Home Secretary and the Commissioner.[83]

These provisions were modeled on the Interception of Communications Act[84] and essentially reprised in the Intelligence Services Act, which also established a Commissioner and a Tribunal.[85] By that time, neither of the two earlier tribunals had ever upheld a complaint. All three tribunals maintained their "perfect" record[86] until the regime was replaced in 2000.[87]

The impetus for change followed the adoption of more far-reaching legislation incorporating much of the European Convention on Human Rights into domestic law. The Human Rights Act 1998 prohibited any public authority from acting in a manner incompatible with the Convention unless legislation left it no other choice. The Act also required that legislation be interpreted as far as possible in a manner consistent with the Convention, allowing for a declaration of incompatibility to be made if there is a divergence.[88] Among other things, when most of

---

[80] *Id.* at Sch 1, ss 2(1)-(2).
[81] *Id.* at Sch 1, s 6.
[82] *Id.* at Sch 1, s 5(1)(a).
[83] *Id.* at Sch 1, s 5(1)(b).
[84] Interception of Communications Act 1985 (UK) ("ICA 1985"), s 7.
[85] ISA 1994, *supra* note 41, at ss 8-9.
[86] It should be noted, however, that while based on confidential communications, the vast majority of complaints appear to have been from persons not under surveillance at all.
[87] The remedies provisions in the ICA 1985, *supra* note 84, the ISA 1994, *supra* note 41, and several other similar acts were repealed by the Regulation of Investigatory Powers Act 2000 (UK) ("RIPA 2000"), ss 65-70, Sch 3, which created a tribunal system with jurisdiction over all intelligence services.
[88] Human Rights Act 1998 (UK) ("HRA 1998"), ss 3-4, 6. The law remains in force until Parliament acts to remove the incompatibility.

the Act came into force in October 2000, it introduced for the first time a right to privacy in Britain. In preparation for this, the Regulation of Investigatory Powers Act (RIPA 2000) had been passed three months earlier, entering into force eight days before the Human Rights Act.[89]

RIPA 2000 created new judicial and administrative oversight provisions; an Intelligence Services Commissioner[90] and an Interception of Communications Commissioner replaced the previous commissioners.[91] In terms of remedies, the Investigatory Powers Tribunal replaced the three earlier tribunals and enjoyed a significantly wider mandate to investigate claims under the earlier legislation as well as the Human Rights Act.[92] The first determination in favor of any complainant was made in 2005, though the only public explanation was that the conduct complained of "was not authorised in accordance with the relevant provisions of RIPA."[93] Compensation was awarded to the (unidentified) joint complainants, and the records in question destroyed.[94] Two further complaints were upheld in 2008,[95] making a total of three out of around 800 complaints upheld in the Tribunal's first eight years.[96]

---

[89] RIPA substantially came into force on 25 September 2000; the Human Rights Act came into force on 2 October 2000.
[90] RIPA 2000, *supra* note 87, at s 59.
[91] *Id.* at s 57.
[92] *Id.* at ss 65-70, Sch 3.
[93] Report of the Interception of Communications Commissioner for 2005-2006 (House of Commons, London, HC 315, 2007), para 39, [hereinafter Report 2005-2006] *available at* http://www.official-documents.gov.uk/document/hc0607/hc03/0315/0315.pdf.
[94] *Id.*
[95] Report of the Interception of Communications Commissioner for 2008 (House of Commons, London, HC 901, 2009), [hereinafter Report 2008] *available at* http://www.official-documents.gov.uk/document/hc0809/hc09/0901/0901.pdf, para 6.5. The number 800 is determined by looking at each of the new cases submitted to the Investigatory Powers Tribunals as outlined in each of "Report of the Interception of Communications Commissioner" for the years 2001-2008. The specific numbers are found under the heading "The Investigatory Powers Tribunal" located in each report. These are available online.
[96] Report 2008, *supra* note 95, at para 6.2; Report 2005-2006, *supra* note 93, at para 37.

At the same time, however, RIPA also significantly *expanded* the state's powers. In addition to regulating communications intercepts and allowing for roving wiretaps, it also provided a statutory basis for surveillance and covert human intelligence sources—the use of undercover officers, informants, and so on.[97] Perhaps most importantly, it significantly expanded the number of agencies authorized to use these powers. When the Act was passed in 2000, nine agencies were allowed to acquire communications data: the three intelligence services, designated police forces, HM Customs and Excise, and the Ministry of Defense.[98] By 2006, this figure had grown to nearly 800 agencies, including 475 local authorities.[99] RIPA thus allows MI5, MI6, and GCHQ to gather intelligence in the interests of national security, but it also empowered, among other things, local authorities to authorize directed surveillance and employ covert human intelligence to protect public health or to assess or collect money owed to a government department.[100] From 2003, the powers of local authorities were restricted to preventing crime and disorder,[101] though some appeared to be continuing to assert broader powers.[102] By 2009, the Chief Surveillance Commissioner (an office previously established under the Police Act but with additional powers under RIPA 2000) reported that law enforcement agencies were granting 16,000 directed surveillance authorizations annually, with a further 10,000 approved by other public authorities.[103]

---

[97] Home Office, Regulation of Investigatory Powers Act, *available at* http://www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers.

[98] Report 2005-2006, *supra* note 93, at para 8; RIPA 2000, *supra* note 87, at s 6.

[99] *Id.*

[100] RIPA 2000, *supra* note 87, at ss 28-29.

[101] *Id.*

[102] Annual Report of the Chief Surveillance Commissioner to the Prime Minister and to Scottish Ministers for 2008-2009 ("Commissioner Report 2009") (House of Commons, London, HC 704, 2009), para 5.5, *available at* http://www.official-documents.gov.uk/document/hc0809/hc07/0704/0704.pdf.

[103] *Id.* at paras 4.7-4.8.

III. THE SURVEILLANCE SOCIETY

Interestingly, these legislative upheavals barely affected the technology that has come to symbolize Britain's approach to surveillance: closed-circuit television (CCTV). There are an estimated 4.2 million cameras in public spaces in Britain, around one for every fourteen individuals, which is by far the highest concentration of such cameras in the world.[104]

Though the use of photographic images in crime control dates back almost to the invention of the camera, the history of CCTV as a technology of surveillance really began with the commercial availability of the video recorder in the 1960s.[105] The early growth in Britain, as elsewhere, was largely confined to the retail sector, with occasional experiments in using CCTV for security on underground railway stations, to monitor traffic flow, or to capture images of groups such as political demonstrators and football hooligans.[106] The first large-scale public system was erected in Bournemouth in 1985 at the time of the annual conference of the Conservative Party.[107] The year before, the Irish Republican Army (IRA) had bombed the conference hotel in an attempt to assassinate Prime Minister Margaret Thatcher.[108] She was not injured but five others were killed; as a result, security at

---

[104] *A Report on the Surveillance Society,* SURVEILLANCE STUDIES NETWORK, (London) Sept. 2006, at 19, *available at* http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf; *cf.* BENJAMIN J. GOOLD, CCTV AND POLICING: PUBLIC AREA SURVEILLANCE AND POLICE PRACTICES IN BRITAIN 1-2 (2004) (arguing that estimating the number of CCTV cameras is a disputed practice, but that the lowest estimates are 1.5 million cameras excluding cameras in small retail stores).

[105] CLIVE NORRIS & GARY ARMSTRONG, THE MAXIMUM SURVEILLANCE SOCIETY: THE RISE OF CCTV 18 (1999).

[106] Clive Norris et al., *The Growth of CCTV: A Global Perspective on the International Diffusion of Video Surveillance in Publicly Accessible Space*, 2 SURVEILLANCE & SOC'Y 110, 111 (2004).

[107] *Id.*

[108] *Id.*

the Bournemouth conference became a high priority.[109] The experience proved atypical, however, and the slow diffusion of CCTV continued in shops and train stations.[110] By 1991, only ten British cities had open street systems in operation, mostly small-scale and locally-funded.[111]

The turning point was the 1993 abduction and murder of the toddler James Bulger by a pair of ten-year-old boys. A grainy still CCTV image, showing him being led by the hand from a Liverpool shopping centre, was broadcast around the nation and published on the front of every newspaper.[112] In the debate over youth crime that followed, Home Secretary Michael Howard announced a "City Challenge Competition" with £2 million of government funding for open-street CCTV systems.[113] After overwhelming demand, three further challenges awarded a total of £85 million for the capital funding of CCTV.[114] By the mid-1990s, CCTV accounted for three-quarters of the government's crime prevention budget.[115]

Debates over whether CCTV "works" in preventing or solving crime continue, but to some extent those debates miss the point. As with the Bulger case, the most important factor appears to be the symbolic value of showing that *something* is being done.[116] Many commentators have puzzled over the British

---

[109] *Id.*
[110] *Id.*
[111] *Id.*
[112] *See generally* DAVID JAMES SMITH, THE SLEEP OF REASON (1994) (telling the story of the Bulgar abduction and murder and how CCTV helped capture the young perpetrators).
[113] Norris, et al., *supra* note 106, at 111-12.
[114] *Id.* at 112.
[115] *Id. See also* NATIONAL CCTV STRATEGY, HOME OFFICE, LONDON, 2007, at 7, *available at* https://www.cctvusergroup.com/downloads/file/Home%20office%20strategy.pdf (showing that from 1993-2003, the trend continued as a further £170 million was made available to local authorities to install CCTV cameras).
[116] Norris et al., *supra* note 106, at 123. *See also* Martin Gill & Angela Spriggs, *ASSESSING THE IMPACT OF CCTV*, HOME OFFICE RESEARCH STUDY 292, 2005, at 63, *available at* http://rds.homeoffice.gov.uk/rds/pdfs05/hors292.pdf.

tolerance for surveillance.[117] As a population, Britons are generally protective of their privacy at home, though unlike their counterparts across the Atlantic that privacy long lacked legal protection. It is suggested that the economic dislocations experienced in the 1980s exacerbated fear of crime in urban centers, and that the threat of terrorism from the IRA increased the public perception of threats posed in public spaces.[118] Periodic successes—such as the Bulger case, the 1999 London Nail Bomber, and the "7/7" London bombings of July 7, 2005—also serve to erode any significant opposition.[119] In what was probably intended to be a reassuring statement, the head of an industry association said that "[p]eople see these cameras as a kind of benevolent father, rather than as Big Brother."[120] Most of the accounts of the use of CCTV in Britain tend to conclude with the helpless observation that CCTV is the means by which politicians can at least give the appearance of fighting crime and terrorism and absent of a radical political shift, any reduction in CCTV usage is highly unlikely.[121] In fact, CCTV is becoming more widespread and more sophisticated. Already the term "closed-circuit" is misleading as it suggests that images are available only to a limited number of monitors on a circuit that is literally closed.[122] Surveillance systems increasingly use networked digital cameras capable of storing data.[123] A growing number are also available to a wider range of viewers. Footage from CCTV is routinely broadcast in televised programmes about crime, and in some cases "CCTV" is streamed live to the Internet. In October 2009, the company "Internet Eyes" announced that it

---

[117] *See* e.g. Jeffrey Rosen, *The Naked Crowd: Balancing Privacy and Security in an Age of Terror*, 46 ARIZ. L. REV. 607, 609-610 (2004).
[118] Norris et al., *supra* note 106, at 121.
[119] *See* NATIONAL CCTV STRATEGY, *supra* note 115, at 7.
[120] Brendan O'Neill, *Watching You Watching Me*, NEWSTATESMAN, Oct. 2, 2006, *available at* http://www.newstatesman.com/200610020022.
[121] Norris et al., *supra* note 106, at 126.
[122] *Dilemmas of Privacy and Surveillance: Challenges of Technological Change* ROYAL ACADEMY OF ENGINEERING, Mar. 2007, at 33, [hereinafter *Dilemmas of Privacy*] *available at* http://www.raeng.org.uk/news/publications/list/reports/dilemmas_of_privacy_and_surveillance_report.pdf at 33.
[123] *Id.*

would begin streaming real-time CCTV images to subscribers who earn points and cash rewards by identifying suspicious behavior.[124]

The increase in observers may be less significant than the ability of new software to analyze footage automatically. Automatic number plate recognition (ANPR) allows a single camera to record the plates of all cars on a busy highway even at night.[125] ANPR is used today to administer the London congestion charge, tracking every vehicle going into or out of central London.[126] Facial recognition systems have been in use for more than a decade with ever-improving accuracy; many governments now require digital storage of passport photographs to facilitate the technology.[127] Gait analysis and other biometric identifiers are also in development.[128] In addition to the identification of persons and vehicles, video analytics makes it possible to flag suspicious conduct, reducing the need for continuous human monitoring.[129] Intelligent Pedestrian Surveillance was first trialed on the London underground in 2003, initially focusing on loitering and potentially suicidal behavior on station platforms.[130] Similar technology now allows CCTV to detect perimeter intrusions and unattended packages, as well as "street crime or deviation from social

---

[124] Jon Henley, *Spot a Crime in Progress on CCTV. Win a Prize!*, GUARDIAN, Oct. 7, 2009, *available at* http://www.guardian.co.uk/uk/2009/oct/07/cctv-surveillance-internet.

[125] *See* An Introduction to ANPR, *available at* http://www.cctv-information.co.uk/i/An_Introduction_to_ANPR and sources there cited.

[126] Transport for London, *What do I Need to Know About the Central London Congestion Charge Camera System?* (Jan. 2011) *available at* http://www.tfl.gov.uk/assets/downloads/CC-Cameras.pdf .

[127] Ayelet Shachar, *Immigration Beyond Territory: The Shifting Border of Immigration Regulation*, 30 MICH. J. INT'L L. 809, 827-28 (2009).

[128] Laura K. Donohue, *Anglo-American Privacy and Surveillance*, 96 J. CRIM. L. & CRIMINOLOGY 1059, 1143 (2006).

[129] *Is There Still Hope for Video Analytics?*, SECURITY DIRECTOR'S REPORT, June 2009.

[130] Mark Henderson, *CCTV to Spot "Odd" Behaviour on Tube*, THE TIMES (London), July 10, 2003 *available at* http://www.timesonline.co.uk/tol/news/uk/article1149614.ece.

norms."[131] Digitization thus makes it easier to store data indefinitely and to search them intelligently. A report by Britain's Royal Academy of Engineering speculates about being able to "Google space-time"—to pinpoint the location of a given individual at a specific time and date.[132]

A. CCTV and Privacy

As indicated earlier, a right to privacy was only incorporated into British law in 2000, well after the government had committed significant resources to CCTV as part of its crime prevention strategy. Most CCTV systems are not covered by RIPA 2000 as they are typically overt and not targeted for a specific operation or investigation, though of course the images captured may be used later for a variety of purposes.[133] The most important regulation initially came under the Data Protection Act 1998. Though it does not mention the word privacy, the Act regulates the use of personal data in accordance with the 1995 European Data Protection Directive.[134] The Act requires that anyone controlling personal information must comply with eight principles. These require that data must be fairly and lawfully processed for lawful purposes; the data must be relevant and not excessive for those purposes, accurate and up to date, kept securely and for no longer than necessary, not transferred outside the European Economic Area unless there is adequate protection, and handled in accordance with the rights of data subjects including, among other things, the right of access to data.[135]

---

[131] Chris Gomersall, *A Closer Look at Video Analytics: Combing Audio and Video Analytics*, GIT SECURITY + MANAGEMENT, Nov.-Dec. 2007, 36, *available at* http://www.ipsotek.com/files/active/0/A_closer_look_at_Video_Analytics.pdf., *see also* Jenny Hogan, *Your Every Move Will Be Analysed*, NEW SCIENTIST, July 12, 2003, 4.

[132] *Dilemmas of Privacy*, *supra* note 122, at 7.

[133] *See* Commissioner Report 2009, *supra* note 102, at para 5.8(d).

[134] *See generally* Council Directive 95/46, 1995 O.J. (L 281) 31 (EC) (outlining the protection of individuals with regard to the processing of personal data and on the free movement of such data).

[135] Data Protection Act 1998 (UK) ("DPA 1998"), Sch 1.

In addition to more limited exceptions, notably concerning the investigation of crime, a broad exception allows the Minister to certify that certain personal data, which may be described generally and prospectively, should be exempted from the principles for reasons of national security.[136] An affected person can appeal to the National Security Appeals Panel of the Information Tribunal, which has broad powers of judicial review and can quash a certificate if the Minister did not have "reasonable grounds" for issuing it.[137] However, what is unclear is how any such person would become aware of the existence of a certificate. Of the seven appeals that have been published, all but one related to suspicions that MI5 was controlling personal data but had refused to confirm or deny it.[138] Four of the appeals were dismissed,[139] but one led to the quashing of a certificate on the grounds that the blanket national security exemption claimed by the Security Service which allowed it to neither confirm nor deny that it held personal data

---

[136] *Id.* at 28.

[137] *Id.* The Information Tribunal replaced the Data Protection Tribunal in 2000. *See supra* notes 79-87 and accompanying text.

[138] *See, e.g.,* Norman Baker MP v. Sec'y of State for the Home Department [2001] (Information Tribunal (National Security Appeals), para 18, *available at* http://www.justice.gov.uk.

[139] Philip Hilton v. Sec'y of State for Foreign and Commonwealth Affairs [undated](Information Tribunal (National Security Appeals)), *available at* http://www.justice.gov.uk/downloads/guidance/courts-and-tribunals/tribunals/information-rights/the-decision/hilton.pdf ; Tony Gosling v. Sec'y of State for the Home Department [undated] (Information Tribunal (National Security Appeals)), *available at* http://www.justice.gov.uk/downloads/guidance/courts-and-tribunals/tribunals/information-rights/the-decision/gosling.pdf; Peter Hitchens v. Sec'y of State for the Home Department [2003] (Information Tribunal (National Security Appeals)), *available at* http://www.justice.gov.uk/downloads/guidance/courts-and tribunals/tribunals/information-rights/the-decision/hitchen.pdf; John Stevenson v. Sec'y of State for the Home Department [2009] (Information Tribunal (National Security Appeals)), *available at* http://www.justice.gov.uk/downloads/guidance/courts-and tribunals/tribunals/information-rights/the-decision/Stevenson.pdf.

was too broad.[140] That decision led a sixth appeal to be withdrawn but with costs awarded to the appellant.[141] The last case was an attempt by Privacy International to challenge the use of CCTV in central London, but was dismissed on a technicality.[142]

In any event, the English courts adopted a narrow definition of personal data that means that many CCTV systems are not covered under the Data Protection Act.[143] The Act defines personal data as data "which relate to a living individual who can be identified" either from those data or the combination of those data and other information likely to come into the data controller's possession.[144] Academic commentary had assumed that the main point of contention would be over the meaning of "identified"[145] but in a 2003 case concerning an investigation by the Financial Services Authority, the Court of Appeal focused on the term "relate to" and held that the Act did not protect all information that merely mentioned a person's name.[146] Instead, personal data had to be relevant to the data subject as distinct from mere transactions in which he or she may have been involved.[147] This included information that was "biographical in a significant sense" or in which the information had the data subject as its "focus."[148] The

---

[140] Norman Baker MP v. Sec'y of State for the Home Department [2001] (Information Tribunal (National Security Appeals), para 113, *available at* http://www.justice.gov.uk.

[141] Mohamed al Fayed v. Sec'y of State for the Home Department and the Sec'y of State for Foreign and Commomwealth Affairs [2002] (Information Tribunal (National Security Appeals)), *available at* http://www.justice.gov.uk.

[142] Privacy Int'l v. Sec'y of State for the Home Department [2009] (Information Tribunal (National Security Appeals)), paras 18-20, *available at* http://www.justice.gov.uk, paras 18-20. In January 2010 the Information Tribunal was renamed the Information Rights Tribunal.

[143] Durant v. Fin. Services Auth. [2003] EWCA Civ 1746, para 27.

[144] Data Protection Act 1998 ("DPA 1998"), s 1(1).

[145] *See e.g.* Scott Rempell, *Privacy, Personal Data and Subject Access Rights in the European Data Directive and Implementing UK Statute: Durant v. Financial Services Authority as a Paradigm of Data Protection Nuances and Emerging Dilemmas*, 18 FLA. J. INT'L L. 807, 816 (2006).

[146] *Durant* [2003] EWCA Civ 1746, para 27.

[147] *Id.* at para 28.

[148] *Id.*

case was understandable on its facts, as the complainant appears to have sought the information not so much to protect his own privacy as to use the information requested as part of ongoing litigation with Barclays Bank "as a proxy for third party discovery."[149] But the implications of the ruling were far wider.

Although the case did not mention CCTV, the restrictive interpretation of personal data was initially interpreted as meaning that unless CCTV was being used to target an individual—that is, depending on the capacities of the system and intent of the operator—captured images that happened to include an individual would not be regarded as personal data for the purposes of the Act.[150] The Information Commissioner issued a guidance note stating that most small businesses using CCTV, for example, were now outside the Data Protection Act entirely.[151] A revised Code of Practice issued in 2008 adopted a broader interpretation that would cover "most" CCTV if it is directed at viewing or recording the activities of individuals.[152]

For many privacy advocates, the emphasis on regulating CCTV through ensuring that it is not covert and is restricting its focused targeting of individuals fails to address the underlying concerns about privacy. It assumes that the problem lies in the occasional abuse of data rather than on the extent to which the *potential* use might force a large number of people to change their

---

[149] *Id.* at para 31.

[150] Steven Lorber, *Data Protection and Subject Access Requests*, 33 INDUS. L.J. 179, 183-84 (2004).

[151] *See e.g. id.* (offering an example of when information crosses the line from protected private information to what contemplates a privacy violation); s*ee also* ROSEMARY JAY, DATA PROTECTION LAW AND PRACTICE 134-36 (3rd ed. 2007) *and* SUSAN SINGLETON, TOLLEY'S DATA PROTECTION HANDBOOK 15-28 (4th ed. 2006).

[152] INFORMATION COMMISSIONER'S OFFICE, CCTV CODE OF PRACTICE (REVISED ED.), 2008, at 5, *available at* http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guide/ico_cctvfinal_2301.pdf.

behavior.[153] In this respect, even dummy cameras—a cheap alternative to CCTV sometimes used to deter crime—may also have privacy implications.[154] Furthermore the notion that one consents to the use of CCTV by entering an area where cameras, or signs stating that cameras are in use, are prominently displayed presumes that alternatives are possible. If there is no way to leave one's house, take public transport, or enter a workplace without having one's image recorded, then the notion of consent is artificial.[155]

The European Court of Human Rights has not ruled on the privacy implications of CCTV generally, but has challenged the use of footage. Late one evening in August 1995, Geoff Peck was captured on camera in Essex wielding a knife, apparently in preparation for suicide.[156] A CCTV operator alerted police who went to the scene.[157] The police quickly determined that he was a threat to no one but himself, detained him on mental health grounds, and ultimately chose not to charge him with an offence.[158] Some of the footage was later aired on national television, however, and a still image—clearly identifiable as Peck—was used in a public relations exercise to demonstrate the effectiveness of CCTV.[159] Having unsuccessfully pursued all domestic avenues, Peck went to the European Court of Human Rights in Strasbourg.[160]

The Court held that photographic monitoring of an individual in a public place does not, as such, violate the right to privacy.[161] Nevertheless, the recording of the data and the systematic or permanent nature of the record may give rise to such

---

[153] Marianne L. Gras, *The Legal Regulation of CCTV in Europe*, 2 SURVEILLANCE & SOC'Y 216, 225-26 (2004).
[154] *Id.* at 226.
[155] *Id.* at 225.
[156] Peck v. United Kingdom [2003], 36 EHRR 41 at para 10.
[157] *Id.* at para 11.
[158] *Id.*
[159] *Id.* at paras 12-20.
[160] *Id.* at paras 1-7, 27-34.
[161] *Id.* at para 59.

considerations.[162] In this case, Peck had not complained of the recording itself but the use to which it had been put, leading to him being recognized by family, friends, neighbors, and colleagues.[163] The broadcast of his image without obtaining his consent or masking his identity was held to be a disproportionate violation of his private life, when compared with the intended end of advertising CCTV and its benefits.[164]

B. CCTV in the United States

In the United States, these questions are generally addressed through the reasonable expectation of privacy test and there appears to be no constitutional barrier to public surveillance. The Supreme Court held, for example, that a person driving on a public road has no reasonable expectation of privacy in his or her movements from one place to another.[165] There is also an implicit assumption of the risk of surveillance by a person being in public. Challenging CCTV generally would require moving away from these doctrines. One possibility, put forward by Christopher Slobogin, would be to emphasize the "reasonableness" component of the Fourth Amendment to ensure that the intrusiveness of CCTV and other surveillance systems is proportionate to the ends being served, implemented through court-determined minimal guidelines.[166] This is an intriguing argument, but seems unlikely to be adopted in the United States given the increasing use of CCTV in public and commercial spaces, and a string of lower court cases

---

[162] *Id.*

[163] *Id.* at para 60.

[164] *Id.* at paras 62-63, 87; *cf.* Bartnicki v. Vopper, 532 US 514 (2001) (holding that the First Amendment protects a radio commentator who broadcasted a conversation recorded illegally by an unidentified third party).

[165] United States v. Knotts, 460 U.S. 276, 281 (1983).

[166] CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 90-118 (2007). *See also* Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213, 236 n.106 (2002).

holding that surveillance by public cameras is not a search within the meaning of the Fourth Amendment.[167]

As in Britain, CCTV spread first in the retail sector but is now quickly moving to wider use in policing and homeland security. The first deployment by police appears to have been two pairs of cameras installed in Hoboken, New Jersey in 1966 and Mt Vernon, New York in 1971; both were soon dismantled as they were seen as expensive and ineffective.[168] Today, elaborate systems are operating in Manhattan, Washington, D.C., and a growing number of other U.S. cities.[169] Since 2003, Chicago has deployed one of the most sophisticated networked systems, linking 1,500 cameras placed by police to thousands more installed by public and private operators in trains, buses, public housing projects, schools, businesses, and elsewhere.[170] Funded in significant part through homeland security grants,[171] Operation Virtual Shield integrates the cameras with the emergency calling system and automatically feeds nearby video to the screen of an emergency services dispatcher after a 911 call.[172] Former Mayor Richard Daley had

---

[167] Peter P. Swire, *Proportionality for High-Tech Searches*, 6 OHIO ST. J. CRIM. L. 751, 755 (2009) (discussing Slobogin's book and the likelihood of adoption by U.S. courts); Afsheen John Radsan, *The Case for Stewart over Harlan on 24/7 Physical Surveillance*, 88 TEX. L. REV. 1475, 1484-90 (2010) (surveying lower court interpretations of Fourth Amendment limits on surveillance).

[168] Robert R. Belair & Charles D. Bock, *Police Use of Remote Camera Systems for Surveillance of Public Streets*, 4 COLUM. HUM. RTS. L. REV. 143, 143 n.1 (1972); Jennifer Mulhern Granholm, *Video Surveillance on Public Streets: The Constitutionality of Invisible Citizen Searches*, 64 U. DETROIT L. REV. 687, 687-88 (1987).

[169] Robert N. Strassfeld and Cheryl Ough, *Somebody's Watching Me: Surveillance and Privacy in an Age of National Insecurity*, 42 CASE W. RES. J. INT'L L. 543, 543 (2010).

[170] William M. Buckley, *Chicago's Camera Network is Everywhere,* WALL ST. J., Nov. 17, 2009, at B7; Fran Spielman, *Eyes Everywhere: City Wants Businesses, Residents to Share Surveillance Video*, CHI. SUN TIMES, July 24, 2008, at 2.

[171] Press Office of the Mayor of Chicago, *Mayor Daley Announces Major Upgrade to Chicago's 911 System*, February 19, 2009, *available at* http://mayor.cityofchicago.org/mayor/en/press_room/press_releases/2009/february_2009/mayor_daley_announces.html.

[172] Buckley, *supra* note 170; Spielman, *supra* note 170.

said that he hoped to have a camera on every street corner by 2016,[173] but later abandoned plans to require every business open more than 12 hours a day to install indoor and outdoor cameras.[174] More recently, New York City announced the Lower Manhattan Security Initiative, based on London's experience and including many of the same features as its "Ring of Steel."[175]

C. CCTV in Canada

Canada provides an interesting counterpoint to the British and U.S. examples. Unlike Britain, laws protecting privacy were in place well before technological advances made video surveillance more effective and efficient.[176] Unlike the United States, those laws were interpreted expansively and internalized by government authorities and the larger public.[177] This combination appears to have slowed the diffusion of cameras in public spaces, at least temporarily.

The Canadian Charter of Rights and Freedoms, which came into force in 1982, established constitutional protections "against unreasonable search or seizure."[178] Comparable to U.S. jurisprudence on the Fourth Amendment, this has been interpreted on the basis of the reasonableness of an individual's expectation of privacy, as well as the reasonableness of the search.[179] The Privacy

---

[173] Fran Spielman, *Surveillance Cams Help Fight Crime, City Says; Goal Is to Have Them on Every Corner*, CHI. SUN TIMES, Feb. 20, 2009, at 22.

[174] *Id.*

[175] Michael Howard Saul, *Bloomberg to Study London's "Ring of Steel"*, WALL ST. J., May 10, 2010, at A21.

[176] The Canadian Charter of Rights and Freedoms, which includes protections against "unreasonable search and seizure" was enacted in 1982—well before the advances in video surveillance described in this Part. This may be contrasted with Britain, where privacy protections were only incorporated in 2000. *See supra* note 89 and accompanying text.

[177] *See generally* CONTESTED CONSTITUTIONALISM: REFLECTIONS ON THE CANADIAN CHARTER OF RIGHTS AND FREEDOMS (James B. Kelly and Christopher P. Manfredi, eds. 2010).

[178] The Canadian Charter of Rights and Freedoms 1982, s 8.

[179] R. v. Kang-Brown [2008] 1 SCR 456, paras 146-48.

Act 1985 regulates the collection, use, and disclosure of information by federal authorities; other relevant legislation is the Personal Information Protection and Electronic Documents Act (PIPEDA) 2000, which serves some purposes comparable to the British Data Protection Act and was similarly inspired by the European Data Protection Directive. Unlike Britain and the United States, Canada for some time resisted a default acceptance of the spread of CCTV. A Supreme Court decision in 1990 stated that "to permit unrestricted video surveillance by agents of the state would seriously diminish the degree of privacy we can reasonably expect to enjoy in a free society."[180]

The issue is also pressed by a series of activist Privacy Commissioners, one of whom proposed the four-prong test adopted in 2004. In determining whether surveillance is reasonable, it should be established that the measure fulfills a specific need, that the measure will be effective in meeting the need, that the loss of privacy is proportionate to the gained benefit, and that there is no less intrusive method to achieve the goals.[181] In addition to formulating general guidelines, the office has taken on specific campaigns. Among other things, it played a role in Google modifying the rollout of its "Street View" feature, which includes images of streets and initially included identifiable individuals and vehicles.[182] Google subsequently undertook to blur faces and license plates, and to delete the original images permanently after one year.[183]

In preparation for the 2010 Winter Olympics, however, Canada announced plans to install around 1,000 CCTV cameras in Vancouver.[184] The report justifying the deployment of the cameras used the word "temporary" 19 times, but there was early

---

[180] R. v. Wong [1990] 3 SCR 36, para 15.
[181] Eastmond v. Canadian Pac. Ry. [2004] FC 852, para 127.
[182] *Google Street View to Expand in Canada*, CBC NEWS, Mar. 22, 2010.
[183] *Id. See also Google's Privacy Breach "Serious"; Research for Street View Program Inadvertently Collected Personal Data, Privacy Commissioner Says,* TORONTO STAR, Oct. 20, 2010, at B1.
[184] Mark Hasiuk, *City Admits Surveillance Cameras Here to Stay*, VANCOUVER COURIER, Apr. 8, 2009.

speculation that a control room was designed to be permanent and that cameras were unlikely to be sold after the Games concluded.[185] One test of Canada's possible divergence from Britain and the United States was whether, after the Olympics, those cameras were dismantled. Early indications suggested that some—but not all—had been.[186] Greece installed some 2,000 cameras for the 2004 Athens Olympics but many were subsequently dismantled or vandalized;[187] a judge ordered that the remainder could be used in future only for monitoring traffic.[188] Three years later the police were fined for using the cameras to monitor student protests.[189] Security for the 2008 Beijing Olympics was accompanied by the deployment of 300,000 cameras around the Chinese capital.[190] In preparation for the 2012 London Olympics, Britain was reported to be studying the Chinese model carefully.[191]

IV. BIG BROTHER IS A BUREACRAT

The U.S. Supreme Court, in the case that found that movements on a public road are not private, considered the argument that improvements in technology would lead to more extensive and intrusive surveillance.[192] Writing in 1983, the Court held that, if

---

[185] *Id.*

[186] Joe Warmington, *77 New Cameras for G20; Eyes in the Sky Installed Ahead of Summit*, TORONTO SUN May 27, 2010, at 4.

[187] Olympic Security Budget Raised, *Daily Mail* May 5, 2004, a*vailable at* http://www.dailymail.co.uk/news/article-296405/Olympic-security-budget-raised.html; Greek Police Fined for Illegal Monitoring, UPI, Oct. 10, 2007.

[188] Hellenic Republic Data Protection Authority, Decision 63/2004 (Nov. 24, 2004), *available at* http://www.dpa.gr/portal/page?_pageid=33,43590&_dad=portal&_schema=PORTAL.

[189] Greek Police Fined for Illegal Monitoring, *supra* note 187.

[190] Cary Huang, *Beijing to Reactivate Olympic Security Plan for Anniversary; Capital Prepares for 60th Birthday of the People's Republic*, SOUTH CHINA MORNING POST, Aug. 24, 2009, at 4.

[191] David Leppard, *Spy Bugs May be Deployed for 2012*, SUNDAY TIMES, June 7, 2009, at 12.

[192] United States v. Knotts, 460 U.S. 276, 283-84 (1983).

such dragnet-type law enforcement practices should eventually occur, "there will be time enough then to determine whether different constitutional principles may be applicable."[193] The notion that courts will have a leisurely opportunity to consider the implications of new surveillance technologies and their use now seems quaint. As this article suggests, it is right and proper that intelligence services should be established by laws that determine their mandate and powers, and provide remedies for when these are exceeded. Such laws are important not only in limiting possible abuse of authority, but also in protecting the agencies themselves from their political masters. At the same time, however, the importance of the turn to law should not be overstated.

If the turn to law essentially means the formalization of existing practices, as it did with the moves to put MI5 and MI6 on a statutory basis, there may be minimal impact on those practices. Indeed, if not written carefully, legislation may in fact *reduce* protections and widen powers when compared to the discreet practices of a "secret" agency. In Britain, this may be seen in the far wider use of surveillance methods not just by the intelligence services and police but hundreds of local authorities. A notorious recent case saw council officials in Dorset obtain telephone records and secretly follow Jenny Paton for three weeks, logging movements of the "female and three children" in their "target vehicle."[194] The surveillance was justified by suspicions—later proven unfounded—that the woman had falsified her address to get her daughter into a nearby school.[195]

Alternatively, if the turn to law comes well after the spread of a new technology, such as CCTV, it may be too late to affect its deployment or use. The spread of CCTV in Britain was, at least in part, facilitated by the absence of meaningful privacy protections. Moves to use biometric identification and build DNA databases

---

[193] *Id.* at 284 (citing Zurcher v. Stanford Daily, 436 U.S. 547, 566 (1978)).
[194] Sarah Lyall, *Britons Weary of Surveillance in Minor Cases*, N.Y. TIMES, Oct. 24, 2009, at A1; Nicola Woolcock, *Mother Sues Council for Spying on Her Family Home*, THE TIMES (London), 6 Nov. 2009, at 17.
[195] Lyall, *supra* note 194.

will be the next frontier in these debates.[196] However, Britain already has one of the largest DNA databases in the world—including samples of around one tenth of the population—and police routinely collect DNA samples from individuals who are arrested but not charged or subsequently acquitted.[197]

Laws matter. Intelligence officials are, in the end, bureaucrats in the sense of being members of a large organization that is intended to operate in accordance with a set of rules. But the laws adopted may be less important than the culture of an organization and the political climate within which it operates. Good laws can support that culture and protect it from the vagaries of politics. Bad laws can hollow out the culture and lay it bare to the winds of political fortune.

Or laws may be irrelevant to the larger issues at stake. In the 2010 general election, Britain's Conservative Party campaigned on a platform of scrapping plans for an identity card that would be linked to a National Identity Register.[198] For the country with the highest concentration of CCTV cameras in the world, which records every car entering and leaving its capital city, and which stores DNA from a growing proportion of its population, this would appear to be a fairly modest issue on which to draw the line.

---

[196] *See* Lisa Madelon Campbell, *Rising Governmental Use of Biometric Technology: An Analysis of the United States Visitor and Immigrant Status Indicator Technology Program*, 4 CANADIAN J.L. & TECH. 99, 99 (2005).

[197] *See e.g.* Criminal Justice Act 2003 (UK), s 10; R. v. Chief Constable of South Yorkshire Police [2004] UKHL 39, para 3. In December 2008, the European Court of Human Rights held that the retention of DNA and other samples from mere suspects was a disproportionate interference with the right to respect for private life. S v. United Kingdom [2009] 48 EHRR 50, para 125. In early 2011 there were proposals to modify the law to allow such samples to be held for three years and then destroyed. Alan Travis, *DNA Profiles to Be Cut in Rollback of State Intrusion*, GUARDIAN, Feb. 12, 2011.

[198] The Conservative Manifesto 2010, *Invitation to Join the Government of Britain*, at 79, *available at* http://media.conservatives.s3.amazonaws.com/manifesto/cpmanifesto2010_lowres.pdf.