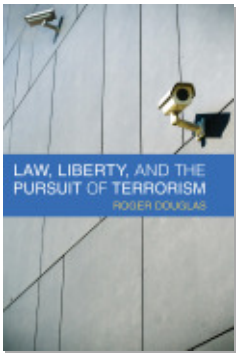
Law, Liberty, and the Pursuit of Terrorism

Douglas, Roger



Published by University of Michigan Press

FOUR

Gathering Information

> Sunlight is said to be the best of disinfectants; electric light the most efficient policeman.
>
> *Louis Brandeis (but not with surveillance in mind)*[1]

> The greatest problem with the Patriot Act may not be that it is unconstitutional, as some argue, but that, in too many respects it is not.
>
> *Susan N. Herman*[2]

> The best friend of prevention is information. If you have the right information you can prevent. Without that information, you can't.
>
> *John D. Ashcroft*[3]

If terrorist conspiracies are to be thwarted, it is almost essential that governments engage in surveillance and almost inevitable that this will involve the surveillance of numerous nonconspirators. This effect is bad enough (although arguably a price to be paid for security), but there is a worse one. National histories disclose long traditions of surveillance targeting "loyal" radicals who want social change but who are basically content to work within the system to achieve it. If those who conducted oversurveillance diligently exonerated nonthreats and turned their attention elsewhere, surveillance might be nonproblematic. But the historical record is discouraging.

First, there are cases where surveillance has thrown up information that is irrelevant to whether the target engages in unlawful behaviour but that nonetheless discredits its target. Governments and their agents have sometimes been unable to resist the temptation to use such information to weaken their political adversaries. Second, while information acquired through surveillance ought to have the potential to exonerate as well as incriminate, there seems to be a bias in favour of looking for evidence that confirms suspicions. This may help explain why agents and governments may believe they are acting properly when they use "irrelevant" information to discredit people whose politics may be objectionable but who are working within the constitution to achieve their ends.

These abuses are well documented, and the political heirs to their victims have long memories. Defenders of surveillance are worried about the errors attending undersurveillance; critics are worried by traditions of oversurveillance. Post-9/11 hindsight lends some support to the advocates of wide surveillance powers, and post-9/11 legal developments provide some support for arguments that the 9/11 attacks spawned unnecessarily broad surveillance laws.

This chapter recognises the obvious: the 9/11 attacks enabled the US government to acquire powers it would otherwise have been hard-pressed to secure. But, I shall argue, the legislation was less ill-considered than the rapidity of its passage suggests. On the whole, the measures were ones that had already been introduced in other countries or were subsequently introduced in calmer times. They fell short of what the administration wanted, as was demonstrated by subsequent administration programs, and they have generally survived constitutional scrutiny. There is little evidence that the 9/11 attacks or others were directly reflected in expanded surveillance powers in the other jurisdictions.

There is ample evidence of the degree to which fondness for surveillance is an executive, rather than a legislative, taste, but this has been manifested not so much in the abuse of powers as in behaviour that appears to have exceeded legal powers. Contrary to what one might expect on the basis of timing and institutional proclivities, courts have generally upheld both surveillance legislation and surveillance practices. Legislative innovations cannot be treated as an opportunistic appeal to popular prejudices. Poll data provide little evidence of widespread popular support for broad surveillance powers either in the immediate aftermath of terrorist attacks or later.

Stances on surveillance reflect political dispositions as well as institutional interests and cultures. Legislative votes on surveillance measures suggest that voting is related to general political dispositions and sometimes more to dispositions than to whether one's preferred party is in government. Poll data suggest a similar tendency among the general public.

Information-Gathering Regimes

Surveillance powers tend to vary depending on whether the information is to be used as evidence in legal proceedings or for security purposes, and there is a grey area reflecting the overlap between law enforcement and intelligence gathering. In the United States, intelligence-gathering powers vary depending on whether the target is a local or foreign adversary. Elsewhere this distinction is less important.

Law Enforcement

Law enforcement agents may collect information in a variety of ways: searches and seizures, interception of communications, analysis of patterns of communication, use of eavesdropping devices, commandeering or asking for records, trawling through rubbish bins, talking to potential witnesses, infiltrating criminal groups, and interviewing suspects. Most (but not all) of these methods require formal authority, especially where they are intrusive or involve interference with privacy. In general, searches, interception, and bugging require warrants from a judicial or quasi-judicial officer, who must be persuaded that there is probable cause warranting their issue. There may also be a requirement that the information is such that less-intrusive information-gathering procedures are impractical. The target of the warrant must normally be notified, either before or after execution of the warrant (depending on its nature). Most jurisdictions now require monitoring of warrants. For some less-intrusive procedures of information collection, administrative subpoenas may suffice, and undercover and public surveillance generally requires no more than administrative authorisation. On the whole, requirements are independent of whether the relevant crime involves terrorism.

These requirements receive considerable constitutional protection. In the United States, the primary basis for such protection is the Fourth Amendment; and section 7 of the Canadian Charter of Rights and Freedoms provides a right "to be secure from unreasonable search or seizure." Under Article 8 of the ECHR, "[e]veryone has the right to respect for his private and family life, his home and his correspondence." Some protection from surveillance and questioning is also provided by constitutional protections of freedom of expression and due process. However, even in the absence of constitutional protections, intrusive surveillance by law enforcement is strictly regulated. This does not mean that it is always in accordance with the relevant law.

There are, of course, variations—over time and place and according to the type of search or surveillance. Warrants of search and seizure normally require probable cause, but in Australia, it is enough that "there are reasonable grounds for suspecting that there is, or that there will be within the next 72 hours, any evidentiary material at the premises."[4] In the United Kingdom, special rules govern search and seizure for the purposes of terrorism investigations. Warrants are needed, but the test relates to whether the material likely to be found will be of substantial value to a terrorist investigation, rather than to whether it is likely to be evidence of an offence.[5]

The requirements for warrants to intercept communications differ from those governing search and seizure. Historically these did not require judicial approval, except where they would otherwise involve trespass.[6] However, ju-

dicial and legislative concerns with protecting privacy interests have resulted in a complex body of law concerned with both restraining and permitting interference with privacy interests. Different jurisdictions have adopted different formulas for doing so. US federal law criminalises the unauthorised interception of any "wire, oral or electronic communication," the use of devices to bug communications, and the use or transmission of details of intercepted communications. However, these activities may be authorised if a judge finds that strict conditions are met, including a nexus between the target, the offence, and the facilities being intercepted or the place of interception, and authorisations must require compliance with procedures designed to protect the communications of third parties.[7] After interception has been completed, the target must normally be given expeditious notification of details of the surveillance.[8] These requirements may be waived in limited circumstances.[9] This does not cover the situation where law enforcement agents seek access to information held by one person and relating to another. These include stored electronic communications (the most important form of which is copies of e-mails held by an Internet service provider). Access normally requires compliance with the search warrant procedures, but after 180 days, the government may give notice to the subscriber or customer. If so, a court may issue an order on being satisfied that the information is "relevant and material to an ongoing criminal investigation."[10]

In the United Kingdom, interception and bugging require warrants, which are issued not by judges but by the home secretary, who must believe that the warrant is necessary for the detection or prevention of serious crime.[11] There is no duty to notify the target. A distinctive but controversial feature of UK law is that it normally prohibits the use of intercepted communications in judicial proceedings.[12]

Canadian law conditions approval of communications surveillance on the judge being satisfied that authorisation would be "in the best interests of justice," and it requires that the target normally be given postsurveillance notification.[13] (In New Zealand, the law was similar until recently.)[14] The normal "last resort" requirement does not apply in the case of terrorism or criminal organisation offences, and the judge may make orders extending the time after which notification must be made for periods of up to three years.[15] Following recent reforms, New Zealand law conditions surveillance warrants on a judge's satisfaction that there are reasonable grounds for believing that surveillance will yield evidence in relation to a serious past, current, or future offence. There is a duty to report to the issuing judge on the outcome of the surveillance, but there is no duty to inform people that they have been the subject of surveillance, unless the surveillance has been in serious breach of the conditions in the warrant or the warrant should not have been issued, and

then only if the judge orders disclosure.[16] New Zealand law makes no special provision for terrorism cases.

Australian law makes separate provision for communications interception, bugging, and access to stored communications. Authorisation for interception requires satisfaction that interception would be likely to assist investigation of a serious offence involving either a person likely to use the relevant service or someone with whom that person is likely to communicate.[17] There are no "last resort" requirements, but issuing officers must exercise their discretion on the basis of proportionality-based reasoning, the existence of less-intrusive alternatives being among the matters to be taken into account.[18] Similar rules now govern access to stored communications.[19] The use of surveillance devices is subject to reasonable suspicion of an offence that is being or will be investigated. Surveillance must be necessary for the gathering of evidence, and the issuing authority must also take account of proportionality considerations.[20] There is no requirement to notify people whose communications have been intercepted.

Laws also permit governments to require that third parties divulge business and other records. Insofar as powers are conditioned on judicial approval, the test for their issuance is typically lower than that for search and seizure and interception orders. In the United States, judicial approval is required for orders that service providers disclose customer and subscriber information, but the test to be satisfied by the applicant is relatively undemanding, and the government is not required to provide the customer a notice of receipt of such records.

UK law permits "authorised" government agents to seek access to communications data.[21] In Canada, judicial officers may order a person other than the person under investigation to produce documents relevant to an offence that has been committed or is suspected of having been committed.[22] In addition, financial institutions may be ordered to disclose account details. Such orders may be issued in relation to future as well as past offences and are conditioned on their promise of assisting investigation, rather than yielding evidence.[23] Australian law allows demands for a range of transactional material. Where the request is in relation to a "serious" terrorism offence, an authorised Australian Federal Police officer may require the production of the information or document. For other serious crimes, however, an application must be made to a federal magistrate.[24] New Zealand law makes no provision for such orders, general search warrants being used as a functional equivalent.[25] However, under legislation in effect from April 2014, orders to produce communications data and stored data may be made by issuing officers who are appointed as such, who may, but need not, be judicial officers.[26]

Subject to a prior authorisation, given on the basis that the authorisation

was "expedient for the prevention of acts of terrorism," the Terrorism Act 2000 gave the United Kingdom the power to stop and search vehicles, drivers, passengers, pedestrians, and anything they might be carrying.[27] Following a successful challenge in the ECtHR to the exercise of these powers, a review of terrorism legislation recommended that the conditions for exercise of the power be replaced with a far more heavily circumscribed power.[28] In accordance with the Human Rights Act 1998, the home secretary made an order limiting the operation of the act, and that order was, in turn, replaced by legislative amendments that sharply limited the scope of the power. The power to make authorisations is now conditioned on reasonable suspicion that "an act of terrorism will take place" and that the authorisation was necessary to prevent such an act and no greater in its territorial and temporal scope than was necessary to do so.[29] Australian law includes a similar provision, with powers generally conditioned on the person being in an area under the exclusive control of the commonwealth and on suspicion that the person has committed, is committing, or is about to commit a terrorist offence.[30] Its scope is therefore circumscribed, although it could catch people in the relevant geographical area who might not fall within the current UK law. Between 2001 and 2006, and after 2013, Canadian law included provision for the making of orders requiring a person to attend for oral examination if there were reasonable grounds for believing that the examination would yield information about a past or prospective terrorism offence.[31]

Intelligence Gathering

Different statutory regimes govern the gathering of intelligence for national security purposes. Typically, these are far less demanding than the criminal law regimes, the justification being that the information is gathered for a different purpose. It is difficult to think of principled reasons why this should be the case, given that intelligence information can be used to assist police with their inquiries and prosecutions. The interests at stake may be higher, but if so, one might expect that this would be reflected in the rules governing law enforcement surveillance. The explanation for the difference seems to lie in practical politics, and in this respect, the relative invisibility of intelligence surveillance may help account for the content of intelligence surveillance law. But it understandably causes unease.

The United States

In the United States, there is little provision for the gathering of intelligence in relation to purely domestic terrorism. Powers in relation to "international"

terrorism are much broader. Various agencies have the power to issue "national security letters" (NSLs), the effect of which is that the recipient must provide relevant information in the recipient's possession. One NSL regime deals with requests for information relating to the leaking of secret government information.[32] The other regimes govern access to various forms of transactional information, including communications transaction records, financial records, and information held by consumer rating agencies about financial accounts. The legislation dates back to 1978. Subsequent legislation expanded the range of information holders who can be asked for and required to provide information, the range of information that can be sought, and the range of people who may seek information.[33] The relevant provisions vary slightly according to the type of records involved.

NSLs do not require judicial authorisation. It is enough that the FBI director or a designated official above a prescribed level certify the existence of facts that would warrant the exercise of the relevant power. The usual requirement is that the records relate to or are sought for "an authorized investigation to protect against international terrorism or clandestine intelligence activities provided that such an investigation is not conducted solely on the basis of activities protected by the first amendment."[34] Other agencies also have the power to require the production of financial records and consumer reports for authorised intelligence-related activities.[35]

Far more important are the powers conferred by the Foreign Intelligence Surveillance Act of 1978 (FISA).[36] Prior to that legislation, the government's power to conduct surveillance for foreign intelligence purposes derived from the president's inherent executive power, the boundaries of which were elusive. FISA was a response to revelations of widespread government surveillance of domestic critics of government policies, coupled with evidence of the misuse of this information. It was predicated on the assumption that it was nonetheless necessary that the United States be in a position to spy on some Americans, either because they were targets or as an unavoidable consequence of the surveillance of non-Americans. Initially, FISA was concerned with communications surveillance. Its scope has been subsequently expanded to permit most of the forms of information gathering open to law enforcement officers.

FISA forbids "electronic surveillance" except as authorised by the act. "Electronic surveillance" is defined to include interception of oral communications, wiretapping, and interception of radio communications. It includes interception of radio communications only in very limited circumstances, and it includes wiretapping and other surveillance only if they impinge on "United States persons" or occur in the United States or if all the senders and recipients are located in the United States.[37] "United States persons" include

citizens, permanent residents, and incorporated and unincorporated associations, unless the corporation or association is a "foreign power."[38] The category of "foreign power" is defined broadly. It includes groups engaged in or preparing for "international terrorism."[39] The category "agent of foreign power" is defined to include, inter alia, anyone who engages in or prepares for "international terrorism." Americans are agents only if they do so intentionally. Electronic surveillance (as defined) is permitted only for the purpose of gathering "foreign intelligence information," which means information that relates to the capacity of the United States to protect itself against attack, sabotage, international terrorism, and clandestine activities by foreign powers or their agents. If information concerns US persons, it is "foreign intelligence information" only if it is necessary to the ability of the United States to protect itself against those threats.[40]

The president, through the attorney general, is permitted to authorise surveillance and searches without the need for a court order, but only if there is little likelihood that this will affect a US person.[41] Otherwise, a court order is normally required. The act provides for a special court, the Foreign Intelligence Surveillance Court (FISC), to consider applications for such orders. The FISC comprises district court judges designated by the US chief justice, and appeal lies with a FISA court of review, comprised of three designated federal judges.[42] Applications to install pen registers and trap and trace devices and for access to business records may also be made to a magistrate judge.

Applications must include a variety of details and certifications, depending on the type of surveillance or information gathering involved. One requirement is certification that the information to be yielded by the relevant process be foreign intelligence information. Its collection must be a substantial purpose where communications interception is involved, and for communications interception and searches, the applicant must certify that there are no less-intrusive ways of getting the information.[43]

Applications for interception, search, and production orders must also include details of "minimization procedures." These are intended to ensure that information about US persons is acquired, retained, and disseminated only as is necessary given the need of the United States to gather foreign intelligence. If information is gathered that is not foreign intelligence information, it shall not normally be disseminated. However, procedures may allow for retaining and disseminating information that is evidence of a crime, for law enforcement purposes.[44]

The judge's role is more limited than that of a judge assessing applications for law enforcement warrants. The judge inquires into whether the application satisfies the formal requirements and includes requisite statements of fact and certifications. It is not for the judge to second-guess the applicant,

except insofar as the judge may find that certifications are "clearly erroneous" on the basis of the material initially presented and further material presented at the judge's request, but then only in relation to interceptions and searches.[45]

Post-9/11 amendments (discussed later in this chapter) have expanded powers to gather and distribute foreign intelligence information. They have also expanded the potential for situations in which law enforcement agencies are unable to gather particular pieces of evidence and information under criminal justice powers but are able to use material gathered under the less-exacting requirements of FISA. However, these apply only in cases where foreign intelligence is gathered. Terrorists who are not acting for a foreign cause have nothing to fear from FISA, except its misuse.

Amendments in 2008 extended the scope of FISA to cover surveillance outside the United States of non-US targets and expanded the circumstances in which surveillance of US persons from outside the United States might be permitted.[46] The purpose of these amendments was not to protect foreign targets (although it does provide them with limited incidental protection). It was to ensure that surveillance ostensibly targeting foreign targets did not intentionally or unintentionally yield an unacceptable amount of otherwise inaccessible information about US persons who might be parties to such communications.

Surveillance of targets outside the United States may now be jointly authorised by the attorney general and the director of national security, but only if the target is not a US person. That power may not be used for the purpose of targeting a particular known person in the United States or to acquire communications involving a sender and recipient who are both in the United States. The exercise of the power must be consistent with the Fourth Amendment to the US Constitution. Authorisation is subject to targeting and minimisation procedures, guidelines, and certification. Procedures and certification must be submitted to the FISC for ex parte judicial review.[47] The amendments subject surveillance of US persons outside the United States to a regime similar to that governing surveillance within the United States.[48] Orders may be made permitting surveillance both within and outside the United States.[49]

The UK Model

The security services of the United Kingdom, Canada, Australia, and New Zealand are empowered to gather intelligence in relation to both domestic and foreign threats. The Canadian, Australian, and New Zealand services were placed on a statutory footing before their UK counterparts (which are now also governed by statute). Their information-gathering powers are sub-

ject to legal regulation and to review. Warrants are required for intrusive information gathering, but the belief requirement relates to the necessity of the warrant for the organisation's performance of its functions, rather than to the likelihood or possibility that those surveilled are engaged in criminal behaviour of which the surveillance might yield evidence. Standards vary according to the type of warrant and cross-nationally. Australian law gives the Australian Security Intelligence Organisation[50] (ASIO) a power not found elsewhere: the power to require people who might be able to provide information about terrorism to answer questions.[51]

There are procedural variations. The issuing authority in the United Kingdom and Australia is the minister (the home secretary in the United Kingdom, the attorney-general in Australia). In New Zealand, warrants require the approval of a warrants commissioner, who must be a former High Court judge, and interception warrants also require the approval of the minister.[52] In Canada, authorisation requires approval from the responsible minister for the making of an application to a judge, as well as authorisation by the judge.[53] In Australia, New Zealand, and the United Kingdom, the process for issuing a warrant is closely monitored by inspectors-general or their equivalent.[54] In the United Kingdom, people who believe that their communications have been wrongly intercepted may complain to the Investigatory Powers Tribunal.[55]

Information gathered by an intelligence service may not be disclosed by the service except in limited circumstances. In Canada and Australia, these include disclosure for criminal justice purposes.[56] In New Zealand, disclosure is permitted in the course of official duties and as authorised by the minister, and the intelligence service's functions include communicating intelligence where this is in the interests of security.[57] These provisions do not expressly permit the use of intelligence information as evidence, but there is Australian and Canadian authority that assumes this to be the case.[58]

Different agencies are responsible for the interception of foreign radio communications and other foreign intelligence. They do not require warrants for intercepting foreign communications, but they do require warrants or authorisation in limited circumstances where a communication involves a citizen or permanent resident.[59]

Surveillance Law and Heightened Fears

Surveillance laws have a complex history. One of their characteristic features is their two-edged nature. To a considerable extent, they both forbid surveillance and permit it. The extent to which they forbid surveillance is not always clear, since statutory prohibitions may coexist with vague constitutional prohibitions and the restraints imposed by other bodies of law, including tort and

property law, privacy law, and state or provincial legislation. To a considerable extent, the impetus for recent pieces of surveillance law has come not from panic in the face of apparent emergencies but from abuses of what were arguably government powers. The evolution of surveillance law has also been influenced by technological developments, which have potential both to facilitate and to complicate surveillance. Moreover, much recent surveillance legislation has been developed contemporaneously with attempts to enhance protections for privacy interests.

Nonetheless, terrorism-related concerns have left their mark on the law, especially in the United States and in minor respects elsewhere. Passed in the immediate aftermath of the 9/11 attacks, the USA Patriot Act[60] strengthened the government's information-gathering powers. One of its most controversial amendments related to the FISA powers regarding seizure of business records. Prior to the 2001 amendments, the director of the FBI or a designee was empowered to apply for an order authorising common carriers, accommodation providers, physical storage facilities, and vehicle renters to provide information concerning international terrorism. This was replaced by a power to apply for an order requiring the production of business records for a FISA investigation.[61] While the section heading referred to "business records," the section itself had the potential to apply to almost any record that might be relevant to an investigation, including, notoriously, library records. Concern about these records was not without foundation. In 1970, the Treasury had indeed sought access to library records with a view to finding out which people were reading books on explosives. The American Library Foundation had staged a successful campaign to discourage cooperation.[62]

Other controversial provisions increased the government's powers to acquire, disseminate, and use information under FISA. The most important of these relaxed the certification requirement for FISA surveillance and searches. Under the law as it stood, the attorney general had to certify that the gathering of "foreign intelligence information" was "for *the* purpose of gathering foreign intelligence" (my italics). Courts had held that this requirement was not met unless intelligence gathering was the "sole or primary" purpose. The amendment relaxed the test to require that the purpose be no more than a "significant" purpose.[63] (The administration had argued that "a purpose" should suffice, but concerns about the constitutionality of the proposal led to adoption of the less expansive phrase.)[64] The precise implications of this amendment would depend on how the word *significant* was interpreted, but whatever its full meaning was in this context, it at least meant that there were circumstances where surveillance was authorised notwithstanding that it was the sole or "primary" purpose for the investigation. This revision increased, in turn, the range of circumstances in which law enforcement agencies might be

able to use FISA procedures to gain evidence that would not be available under criminal justice procedures.

Other amendments to the FISA powers were less wide-ranging. The power to make ancillary orders in relation to surveillance was expanded so that orders could be made against nonspecified persons when the actions of the target of the surveillance might have the effect of thwarting attempts to determine the person's identity.[65] Unlike similar law enforcement powers, the applicant did not have to specify the target's identity: a description could suffice. Nor was there a requirement that the person subject to surveillance be notified after the expiry of the surveillance. The Patriot Act also expanded the maximum duration of orders.[66]

The act expanded the range of FBI agents who could request transactional records.[67] Providers' powers to disclose stored information were expanded to permit otherwise forbidden disclosure when there was reasonable belief that disclosure was required by "an emergency involving immediate danger of death or serious injury to any person." In 2002, the emergency power was expanded still further.[68]

The act made minor amendments to the law governing criminal investigations. The power to seize stored electronic communications was expanded so that it included voice mail.[69] The details of information that could be subpoenaed were extended to include details of the means and source of payments.[70] The law governing pen registers and trap and trace devices was amended to make it clear that it applied to Internet, as well as more traditional, communications. Requirements for authority to use pen registers and trap and trace devices were changed so that they could have nationwide application and such that the communications to which they related could be defined with less particularity than had previously been the case.[71] The Federal Rules of Criminal Procedure were amended so that search warrants in relation to investigations of domestic and international terrorism could be sought in any district in which activities related to the terrorism might have occurred, for searches both inside and outside the district.[72] Provision was also made for nationwide service of search warrants for electronic evidence.[73]

The act expanded the disclosure powers of law enforcers who had obtained foreign intelligence information in the course of lawful surveillance information, so that they could disclose it to federal officials for the purposes of assisting them in their official duties.[74] Relevant information otherwise obtained in the course of a criminal investigation could be similarly disclosed.[75] The act amended the Federal Rules of Criminal Procedure to permit the disclosure of matters occurring before a grand jury to a variety of federal officials, for the performance of their official duties, in cases involving national security or international or domestic terrorism (as defined in 18 USC § 2331).[76]

One amendment, which has survived in modified form and notwithstanding its apparent unpopularity with the public, allowed a judge to dispense with the requirement that a person whose premises had been searched be notified within a specified time. The FBI had made earlier, unsuccessful attempts to secure this power.[77] Its rationale was clear: to avoid tipping off the subject of the investigation. The power was not confined to terrorism cases.

Several attempts were made in the US House of Representatives and the Senate to delete some of these measures. They failed by sizeable majorities, especially in the Senate.[78] The act was passed by a large majority in the House and with only one dissentient in the Senate. The act and its history exhibit many outward signs of being both a response to heightened fears and a reform that was particularly ill thought through. Its name and timing are suggestive. It was passed in considerable haste in the immediate aftermath of the 9/11 attacks and the even more immediate context of the anthrax scare. Browbeaten by threats that unless it moved quickly, it might well have blood on its hands, the Congress bypassed and abbreviated normal procedures and passed the legislation within a month of being presented with the administration proposals. Members of Congress complained that they had been unable to track down copies of the latest versions of the legislation, much less to study them. (One reason was that following the anthrax attacks, Congress's administrative infrastructure had been temporarily impaired.)[79]

It is useful to disentangle various elements of the "haste" perspective. First, while the legislation was passed in almost indecent haste, neither the executive nor the Congress was completely unprepared for the legislation. Orin Kerr points out that the Department of Justice "had been clamoring for changes to the antiquated surveillance laws for years"[80] and that the Clinton administration had already proposed some of the changes implemented by the act. Indeed, in 1995, following a series of terrorist bombings, the House Judiciary Committee had endorsed, by majority, an act that, if passed, would have included some of what resurfaced later as Patriot Act provisions. Nonetheless, the fact that these proposals had hitherto failed to commend themselves to Congress suggests that the 9/11 attacks provided their proponents with an opportunity to secure the passage of legislation that would normally have been doomed.

Second, post-9/11 emotions notwithstanding, Congress did not give the administration everything it wanted. In the immediate aftermath of the attacks, the attorney general was urging Congress to pass the administration's proposals within a week, notwithstanding that they had not yet been drafted. His major defence of the administration's proposals lay in warnings about the present danger rather than in explanations of why the proposals would avert them.[81] But Congress refused to agree to several of the more objectionable

features of the administration's proposals, notably in relation to the use in US courts of material provided by foreign surveillance agencies, the range of officials who might have access to criminal justice and national security information, the ease with which sneak and peek warrants might be obtained and their scope, the conditions for access to business records, and the scope of and accountability for powers in relation to pen registers and trap and trace devices.[82] Moreover, in face of administration objections,[83] most of the Title II Patriot Act amendments to information-gathering powers were subject to sunset provisions.[84]

Further, insofar as there was panic, it was by no means general. The administration's call for almost instantaneous passage of its proposals did not prevail. In the House, the Democratic minority resisted attempts to expedite the passage of a bill that many of them regarded as inferior to one that had received the unanimous support of the House Judiciary Committee. There was some apocalyptic language used to defend calls for urgent passage of the legislation, but it was the exception. Much of the House debate involved Democrats challenging the need for urgency, and many cited past abuses of surveillance powers. In the Senate, defenders of the legislation often combined arguments that it should be passed with awareness of past abuses and took comfort from the thought that the sunset clause would enable reconsideration in calmer circumstances. However, the Democratically controlled Senate voted 98–1 for the legislation, and the House voted 337–97 in favor.

The surveillance provisions faced and continue to face strong opposition. They have been the subject of critical resolutions passed at state, city, and town level. In 2003, the proposed Freedom to Read Protection Act failed by a tied vote to pass the House of Representatives.[85] In 2005–6, Congress once more considered the act. Since most of the Title II provisions had been subject to a sunset clause, they could have been allowed to lapse. Instead, in 2006, the sunset provisions were removed except in relation to the "roving wiretap" and business records amendments, whose expiry date was advanced to 31 December 2009.[86] But the legislation limited the sneak and peek power, by dropping delay to trial as a sufficient ground for such warrants, presumptively limiting their duration to 30 days and renewals to 90 days, and by requiring reports to the Administrative Office of the United States Courts and to Congress.[87] The same legislation limited the range of officials who could apply for certain records, including records relating to library use, book sales, tax, education, medical treatment, and firearms sales. It also made provision for judicial review of production orders and added minimisation requirements.[88]

In late 2009, the expiry date for the business records power was extended until 28 February 2010.[89] There was considerable division within Congress as to whether some or all of the amendments should be repealed, amended,

or allowed continued operation and, if so, for how long.[90] The solution was a compromise, suggesting considerable lack of enthusiasm for the amendments: their operation was subsequently extended until 28 February 2011.[91] In February 2011, their operation was extended until May, and it was subsequently extended for another four years.[92] The survival of most of the Patriot Act amendments suggests that their passage cannot be explained simply in terms of temporarily heightened fears, but the uneasy fate of several of the amendments suggests a degree of support for this perspective: their survival has been dependent on their being slightly "weakened" and on the continuation of the sunset clause.

Postattack fears appear to have made little impact on surveillance legislation elsewhere. In the United Kingdom, the power to stop and search suspected terrorists in designated areas predated 9/11. It had its origins in measures designed to deal with the problem of Irish terrorism, but its presence in the United Kingdom's comprehensive Terrorism Act 2000 cannot be understood as a reaction to a particular attack, given the four-year gestation period that preceded the legislation and given that it was enacted in a climate in which the threat of Irish terrorism seemed at last to be ebbing, while the threat of terrorism from elsewhere was diffuse. The Regulation of Investigatory Powers Act 2000 (c 27), which governs most forms of surveillance in the United Kingdom, was prompted by the need to make UK legislation compliant with ECHR standards, although it also permitted surveillance in some circumstances in which it was not permitted under earlier guidelines.[93] The Anti-terrorism, Crime and Security Act 2001 (c 24), which was passed on 14 December 2001, included one surveillance-related innovation. Part 11 of the act made provisions for procedures whereby the home secretary could require telecommunications companies to retain communications data for national and crime control purposes.

Australia's suite of post-9/11 measures included several provisions dealing with surveillance issues. The most controversial related to ASIO's new power to question and require answers from people in possession of terrorism-relevant information. This met considerable resistance and was not passed until 2003, in an amended form.[94] The only other measure relating to surveillance was a bill dealing with stored communication. The issue the bill sought to address had virtually nothing to do with terrorism and was not finally resolved until 2006 (in a manner that differed from that proposed in 2002). Its effect was to strengthen protections for stored communications. A 2008 bill that would have empowered ASIO to apply for warrants to intercept communications involving named persons, without the need to specify the instruments to be intercepted, attracted cross-party opposition in the Senate and

was dropped. A compromise relaxed the requirement for warrants for named persons so that a single warrant could specify multiple communication devices. The power to conduct roving wiretaps remains one of the few powers enjoyed by US agencies but not by ASIO.

Following the London 7/7 attacks, the Council of Australian Governments reviewed terrorism legislation. Eight of the nine jurisdictions agreed on a wide-ranging package of measures that included provision for added terrorism-related surveillance powers.[95] The most important of these provided that an authorised Australian Federal Police officer who believed, on reasonable grounds, that a person had transactional records that would assist the investigation of a "serious terrorism offence" could give the person a notice requiring the production of the documents.[96] The other provided for stop and search powers, along the lines of the UK powers, but far more circumscribed in relation to the areas in which they could be exercised.[97] Witnesses before the Senate committee that considered the bill were almost unanimously opposed to the amendments, but the committee recommended its passage subject to minor amendments, including a sunset clause expiring in 5 years rather than 10. The government declined to follow this recommendation. The surveillance measures were passed without further amendment and with little debate, the surveillance issues being overshadowed by far more controversial features of the bill.

General developments in Australia's surveillance law were largely uninfluenced by terrorism-related concerns. Debates, Senate reports, and government papers make no more than occasional, oblique references to terrorism. ASIO's surveillance powers remained almost unchanged during the post-9/11 years.

Canada's post-9/11 legislation amended the requirements for communications interception so that if there was a terrorist offence, the "last resort" requirement did not have to be satisfied, and the target did not have to be notified of the existence of the interception. Further, the target of an interception authorisation did not have to be informed within 90 days of the giving of the authorisation.[98] Potentially more important were provisions for the compulsory questioning of people believed to have information about past or future terrorism offences. Unusually, this legislation was subject to a sunset clause, and expired after the Parliament failed to pass a resolution extending its operation. It was revived in 2013. Otherwise, Canadian surveillance legislation has remained largely unchanged, and there have been no relevant changes to the surveillance powers of the Canadian Security Intelligence Service.

In 2003, New Zealand followed Canada in making special provision for interception of communications in terrorism cases, but the difference between

terrorism cases and other cases was negligible.[99] Following a Supreme Court decision[100] whose practical effect was that police lacked the power to gather video evidence except when surveillance was from a public place, the government introduced legislation to validate the use of covert video surveillance from outside an area under surveillance or in conjunction with an authorized search. The legislation applied retrospectively but not to the successful Supreme Court appellants. Its purpose was not to assist the prosecution of suspected terrorists (although it has arisen in a "terrorism" case) but to foreclose the collapse of other pending trials.[101] The following year saw the passage of the comprehensive Search and Surveillance Act 2012, in which the minimal distinction between terrorism surveillance and other forms of surveillance disappeared. Terrorism concerns appear to have been irrelevant to the formulation of the new legislation.[102]

One reason for the different responses of the United States and the other four countries may lie in the particular intensity of the fears and passions unleashed in the United States by the 9/11 attacks, but another may be the many respects in which the other four governments already enjoyed powers conferred by the Patriot Act amendments. Even after the FISA amendments, the FBI's intelligence-gathering powers are narrower in some respects than those of the other countries' security services. In general they are available only for investigations of international terrorism, although this limitation has proved of only limited importance. Many of the FISA powers require judicial approval, whereas security service powers in the United Kingdom and Australia are conditioned on ministerial approval. The new powers to communicate foreign intelligence information to people involved in law enforcement were no greater than those enjoyed by security services elsewhere (although intercept information continues to be unavailable in the United Kingdom as evidence in trials). The controversial power to gain access to business records was already enjoyed by the security services. That said, there are some respects in which US surveillance powers are broader than surveillance powers elsewhere. Unlike the United States, Canada and New Zealand require approval from a judge or retired judge for demands for transaction data in security-sensitive cases, and the United States roving warrant provisions are more generous than the equivalent Australian provisions.

Governments and Surveillance

Surveillance legislation usually involves legislative resistance to proposals to expand government powers, and there appear to be no examples of legislatures conferring greater surveillance powers on the government than the government had sought. Even when voting for the passage of the Pa-

triot Act, legislators were worried about government abuses and cited the well-documented examples of law enforcement agencies' willingness to act with little regard for both law and political proprieties.[103] The United States is not, of course, unique. It was almost an open secret that Australia's largest state police force engaged in phone tapping for more than a decade when it had no authority to do so under the law.[104] The Canadian royal commission investigating the surveillance activities of the Royal Canadian Mounted Police pointed to a long history of improper and illegal surveillance.[105]

The frequency of these forms of deviance is testimony to the avidity with which police and intelligence agencies pursue the acquisition of information. The past is not necessarily a guide to the present. Enhanced surveillance powers may reduce the perceived attractions of deviance. Organisational cultures may change in response to the difficulties of getting away with unlawful surveillance. But intelligence agencies and police continue to press the limits of their legal powers and sometimes still exceed them.

United States

In the United States, there is evidence that the executive has made increasing use of its powers. Despite their expanded powers, officials have engaged in surveillance without complying with prescribed pre-conditions for doing so, but bureaucratic and legal imperatives have set some limits to the level of surveillance.

Use of Powers

The United States provides information about the use of national security letters, the number of applications for FISA interception and/or search warrants, and the number of applications for orders for the production of records and tangible things. These statistics indicate that the use of NSLs has tended to increase since 2001, that there was a steady increase in FISA warrants up to 2007, and that applications for orders for records have been infrequent but sharply increased to 96 in 2010. On the whole, published statistics are unhelpful. They indicate that the likelihood of a randomly selected American being subject to these forms of surveillance is small (about 1 in 20,000 in relation to NSLs), but they leave open the question that matters: whether and to what extent the surveillance provided useful information.[106] Use of roving wiretaps has also been limited. By March 2009, they had only been approved on 147 occasions, but on only one of these occasions does their use seem to have disrupted a terrorist plot.[107]

Exigent Letters

The criteria for issuing national security letters are considerably more relaxed than those relating to the access to content. But between 2002 and 2006, FBI agents in the Communications Analysis Unit (CAU) and (to a lesser extent) the New York Field Division regularly bypassed the statutory requirements, along with guidelines governing requests for call data. A widespread practice involved the use of "exigent letters," requesting call information and stating that formal process would be served subsequently: at least 798 such letters were issued between 2003 and 2006, 722 from the CAU.[108] Investigations by the Department of Justice's Office of the Inspector General found numerous irregularities surrounding this practice. These included the absence of exigent circumstances, the lack of a statutory basis for such letters, their use by people who lacked the power to issue NSLs, their use to gather information for purposes other than national security purposes, failures on behalf of those issuing them to specify time limits to the information sought and to set in motion procedures for ensuring that NSLs would ultimately issue, and failure to monitor their use.[109] Letters were also used to obtain information about subsequent use of communications services.[110] Representatives of the phone companies sometimes prepared NSLs for the FBI.[111]

There was also evidence of exigent letters being issued in the context of the investigation of leaks, requesting call data relating to journalists' phones, without regard to whether this was consistent with the express statutory prohibition on the issue of NSLs in relation to activities protected by the First Amendment and in contravention of the procedures prescribed by regulation.[112] The inspector general also found evidence of informal requests for information by e-mail, phone, and face-to-face communication.[113] A review of a small sample of FISA requests found a number of instances where officials swore that relevant call data had been obtained by NSL when this had not been the case.[114]

Those who signed the letters generally seem to have assumed that the procedure was lawful, guiding their practice by unit folklore and advice from the phone companies rather than by reference to law or to manuals embodying the law. When signatories did express concern, they were assured that "lawyers" had approved the letters. Senior officials were either unaware of the practices or assumed that they were lawful. Service providers were remarkably cooperative, often (but not invariably) taking FBI emergency claims on trust.[115] Even lawyers for the National Security Law Branch (NSLB) seemed unconcerned that exigent letters might be unlawful. They were aware of and concerned about increasing delays in the process of issuing the NSLs promised in exigent letters, but they seem not to have realised that NSLs could not

confer retrospective validity on exigent letters. By 2004, doubts were increasing. The NSLB assistant general counsel (AGC) considered that emergency letters might be issued only for periods of up to 48 hours and that applications for subsequent NSLs should not be written to conceal the existence of the prior letters. Despite being aware of these problems, the deputy general counsel continued to apply for NSLs months after the relevant exigent letters and without making reference to their existence.[116]

The NSLB's assumption that there was a power to issue exigent letters was not based on the text of the statute. The AGC's analysis was that "the FBI had 'tried to reconcile the literal interpretation . . . with lots of other policy considerations' that the FBI needs to deal with when 'lots of lives are at stake.'"[117] As late as May 2005, the AGC had not actually seen a copy of an exigent letter.[118] Moreover, given express statutory provision for emergency requests for the provision of data, the assumption underpinning exigent letters seems implausible (and the inspector general found it to be).

Further, in response to providers' concerns about the delay in providing promised NSLs, the CAU issued a series of blanket NSLs. Not only could these not operate retrospectively, but they also failed to meet several of the statutory requirements for NSLs. Some related to crime as well as national security interception. None mentioned that the details had been sought and provided. Most did not include the certification required when NSLs included a confidentiality requirement.[119]

President's Surveillance Program

Unlike some questionable surveillance programs, the President's Surveillance Program (PSP) was conducted with the knowledge and authority of the president. The program was first authorised shortly after the 9/11 attacks, for a period of 45 days, and was subsequently extended by further 45-day extensions.[120] From 25 October 2001, briefings on the program were given to congressional leaders and their staff[121] and to two members of the FISC.[122] Its full scope is still partly classified. One of its elements was the Terrorist Surveillance Program (TSP). Under the program, the National Security Agency (NSA) was purportedly empowered to "intercept the international communications of people with known links to Al Qaeda and related terrorist organizations." Interception was conditional on at least one party to the communication being outside the United States and on at least one party being associated with al-Qaeda or a member of an affiliated organisation. Surveillance took place on a massive scale. Up to 500 phone conversations were simultaneously monitored, and spying extended to millions of Americans' phone calls and e-mails.[123] Its operation was dependent on the voluntary cooperation of tele-

communications companies.[124] The TSP was supplemented by "other intelligence activities," details of which remain classified.[125]

Until 2004, the Office of Legal Counsel (OLC) of the Department of Justice (DOJ) advised as to the legality of each successive authorisation, and the attorney general certified as to the legality of the program.[126] Certification required grounds for reconciling the program with the language of FISA. John Yoo, deputy assistant attorney general and the only OLC official read into the program, rose to the challenge, arguing that FISA was to be read as not applying to emergency surveillance and that insofar as FISA purported to do so, it represented an unconstitutional infringement of the president's Article II powers. The only limit on these powers was the Fourth Amendment, and insofar as it was applicable, it required no more than that the surveillance be reasonable. In the circumstances, this requirement was satisfied.[127] In 2003, Yoo resigned, and two other DOJ officials (Patrick Philbin and Jack Goldsmith) were read into the program. They were concerned about flaws in Yoo's analysis, and the deputy attorney general, James Comey (who was also read into the program), agreed. The White House counsel, Alberto Gonzales, disagreed and argued that thousands of lives would be at risk if the program was not recertified. Conflict between the DOJ and the White House culminated in an episode one might expect in a political thriller, the two sides descending on the hospital where the attorney general, John Ashcroft, was recovering from surgery. The White House representatives tried to persuade the ailing Ashcroft to sign the reauthorisation. He refused, citing his reservations and then adding that his views did not matter, since his powers currently lay with his deputy.[128] The solution was a reauthorisation certified by the White House counsel, which the DOJ interpreted as being binding on the entire executive branch, notwithstanding that it was based on a flawed analysis of the law. The White House continued to insist that the law was on its side, but it dropped some of the activities that the DOJ had found to be unlawful.[129]

Surprisingly, the existence of the program was kept relatively secret until about 2005, and the last authorisation expired on 1 February, following a successful application by the government to the FISC for a warrant authorising surveillance of communications of the type authorised under the TSP but subject to the FISA minimisation requirements.[130] Two issues were left to Congress to resolve: (1) whether there should be any protection against legal liability for corporations that had cooperated with the program and (2) the circumstances in which the government might be permitted to intercept communications when the interception took place outside the United States or involved a non-US person as a target.

The initial congressional response was the Protect America Act of 2007.[131] The act amended FISA by excluding surveillance from the definition of "elec-

tronic surveillance" if it was "directed at a person reasonably believed to be located outside the United States."[132] This meant that such surveillance was permitted. It also provided a mechanism whereby the government could acquire foreign intelligence information from others who might have access to it.[133] The price for its passage was an extremely short sunset period, on whose passage the legislation lapsed. It was followed by the FISA Amendments Act of 2008,[134] passed with the support of Republicans and a minority of Blue Dog Democrats.[135] This legislation subjected electronic surveillance targeting people outside the United States to a regime subject to FISC supervision. It also made it clear that surveillance was permitted only insofar as it was permitted under FISA or some other statute.[136] The FISA Amendments Act also protected the telecommunications providers from civil liability and state inquiries arising from their cooperation with the government.[137]

United Kingdom, Canada, Australia, and New Zealand

Elsewhere, executive deviance seems to have been more restrained. However, the United Kingdom's use of stop and search powers provides evidence that counterterror powers can be misused or, alternatively, that the purported exercise of those powers is sometimes for improper and therefore unlawful purposes. The stop and search powers were meant to be used in relation to suspected terrorism. By 2010, there was evidence that the power was being used other than for its intended purposes. The areas approved as areas in which people might be stopped included areas where there was no reason to believe that stopping people could serve a counterterrorism purpose. People were sometimes being stopped not for investigative purposes but to produce statistics consistent with nondiscriminatory law enforcement. The annual incidence stoppages in London had increased to 185,086 by 2008–9. While exercise of the power had yielded evidence to ground a small number of convictions for nonterrorism offences and a small number of arrests for terrorism, no terrorism conviction had ever resulted from an exercise of the power. In 2009–10, far fewer people were stopped (80,309 in London), and only 0.5 percent of stops resulted in arrests, none of which were for terrorism offences.[138]

Reports by the interception of communications commissioner provide no information about the number of security-related warrants and only limited details of irregularities relating to security service warrants.[139] They give details of errors reported to the commissioner, which all appear to have involved human error rather than deliberate abuse. They include assurances that inspections of security-related warrants indicate that the agencies have been complying with the act and the code of practice. Reports of the intelligence services commissioner suggest satisfaction with the performance of the sec-

retaries. "Outright and final refusal of [applications] is comparatively rare," according to one report, but senior officials sometimes seek amendments, and the secretaries sometimes require further additional information.[140]

Reports by the Australian inspector-general of intelligence yield similar results. The inspector-general aims to review all warrant requests on their merits, as well as for formal compliance, and to check files to ensure that interception takes place only pursuant to warrant. Annual reports have been positive, although reports mention an average of three cases per year where fault or error led to unlawful interception and a somewhat greater number where there was the unrealised potential for such interception.[141] As in the United Kingdom, these typically involved mistranscriptions and phone numbers that had been reassigned to a person of no security interest, but there were two cases where action purportedly based on a warrant was initiated before the attorney-general had actually signed the warrant.[142] There were no reported cases of deliberate unlawful surveillance. Annual reports from New Zealand's inspector-general give details of the number of warrants issued each year (about 20). They report no irregularities. However, New Zealand's High Court and Supreme Court found that video surveillance of the training camps of suspected domestic terrorists had been unlawful.

Institutional Proclivities: Courts

United States

Underlying the PSP was mistrust of the courts, including the FISC. Jack Goldsmith quotes David Addington, the vice president's counsel, as saying, "We're one bomb away from getting rid of that obnoxious court,"[143] and the reluctance to try to put the PSP on a sound legal foundation reflected this suspicion. However, on the whole, courts have placed few obstacles in the path of government surveillance. FISA applications have almost invariably succeeded. Only about one in a thousand is denied, although FISC made substantive alterations to proposed orders in about 4 percent of cases between 2003 and 2010.[144] Published statistics do not reveal whether judges (or retired judges) in Canada and New Zealand are as cooperative, but statistics relating to criminal justice warrants and approvals suggest a similarly high success rate. Applications for law enforcement warrants succeed in more than 99 percent of cases. Challenges to the legality of surveillance have had some, limited success. In the United States, a long series of Supreme Court decisions had already limited the scope of Fourth Amendment protections,[145] and the Fourth Amendment made little impact on the outcome of post-2001 terrorism surveillance cases.

The Constitutionality of FISA

Challenges to the constitutionality of the FISA legislation have been numerous and, with one arguable exception, unsuccessful. Indeed, prior to the enactment of FISA, there was considerable authority to the effect that the president had inherent (but not unlimited) power to conduct warrantless surveillance for foreign intelligence purposes in certain circumstances.[146] Moreover, while the Supreme Court has not yet pronounced on the validity of the legislation, it has accepted that even if surveillance legislation did not require a warrant on probable cause, "standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of government for intelligence information and the protected rights of our citizens."[147] This observation underlay rulings that FISA, as enacted, was constitutionally valid even if FISA warrants fell short of Fourth Amendment warrant requirements. However, these decisions left open the question of whether the 2001 amendments to FISA were constitutional.

In March 2002, the attorney general approved new "intelligence sharing procedures," following the Patriot Act amendments to FISA, and filed a motion with the FISC seeking an order that it vacate pre-2001 orders in which it had adopted more-demanding minimisation procedures. In May 2002, the presiding judge of the FISC ordered that the new procedures be adopted, with modifications, to apply as minimisation procedures operating in all cases. These precluded law enforcement officials giving recommendations to intelligence officials in relation to FISA searches or surveillance, and the requirement that the FBI and the Criminal Division of the Department of Justice take steps to ensure this. The decision was reissued following argument before all the members then serving on the court. The government then appealed to the Foreign Intelligence Surveillance Court of Review, which allowed the appeal.

In *In re Sealed Case No 02–001*, the court of review held, first, that the FISC's decision had been based on a misconception that there was a dichotomy between law enforcement and intelligence gathering. Information was to be gathered as a means to an end, the protection of US interests, and this end might sometimes be one best achieved by a criminal prosecution.[148] The court found, second, that the conditions imposed by the FISC did not answer the description of minimisation procedures. These were intended to minimise the misuse of information that was not "foreign intelligence information." Since the legislation permitted the retention of information that was not foreign intelligence information if it was evidence of ordinary crimes, using it for this purpose did not constitute misuse. Moreover, the FISC had erred by failing to take account of the implications of the Patriot Act amendments.[149]

The court of review considered that the Patriot Act amendment implied

the existence of the very dichotomy that the court had found not to exist under FISA as enacted. But the court interpreted the amended legislation as allowing the use of FISA powers to gain foreign intelligence information except where the sole purpose for doing so was criminal prosecution. This qualification would rarely matter: when the government "commences an electronic surveillance of a foreign agent, typically it will not have decided whether to prosecute the agent (whatever might be the subjective intent of the investigators or lawyers who initiate an investigation)."[150]

Recognising that the broad interpretation of the surveillance powers raised serious questions as to their validity, the court considered two questions: whether the orders constituted warrants for the purposes of the Fourth Amendment and, if not, whether they satisfied the "reasonableness requirement." The court concluded that FISA orders might not be warrants as contemplated by the Fourth Amendment. The probable cause requirement was weaker than for law enforcement warrants, as were important aspects of the particularity requirements. But, it was relevant to satisfaction of the reasonableness requirement that the legislation came close to satisfying the warrant requirement. Also relevant were the public interests at stake, a consideration recognised by the Supreme Court in *United States v United States District Court (Keith).*

The court recognised that there was a Fourth Circuit authority in *United States v Truong Dinh Hung,* to the effect that nothing less than a "primary purpose" requirement could be "reasonable" for Fourth Amendment purposes.[151] *Truong* related to pre-FISA law but had implications for the validity of FISA. The court of review concluded that *Truong* was based on untenable assumptions. The artificial distinctions that it drew generated "dangerous confusion" and created "perverse organisational incentives."[152] It created walls where "effective counterintelligence, we have learned, requires the wholehearted cooperation of all the government's personnel who can be brought to the task."[153] The Supreme Court had approved "apparently warrantless and even suspicionless searches that are designed to serve the government's 'special needs, beyond the normal need for law enforcementn'"[154] The court of review emphasised that the threat facing America could not be forgotten: "After the events of September 11, 2001, though, it is hard to imagine greater emergencies facing Americans than those experienced on that date"; "Our case may well involve the most serious threat our country faces."[155]

Subsequent decisions have almost invariably followed *Sealed Case.* While courts have sometimes preferred to deal with admissibility issues by finding that FISA evidence would have satisfied the "primary purpose" test, their language suggests that they have done so out of caution rather than out of doubts as to whether FISA, as amended, can survive constitutional scrutiny.[156] Others have made positive findings to the effect that the legislation is valid, some-

times in conjunction with findings that the evidence satisfied the "primary purpose" test,[157] but sometimes not.[158]

The one exception is a 2007 decision, *Mayfield v United States*,[159] where Judge Ann Aicken held that the legislation was unconstitutional. According to Aicken's interpretation, the legislation meant that law enforcers could bypass the more rigorous standards that traditionally governed warrants for law enforcement purposes—namely, the requirements of probable cause, notice, specificity, and short duration. Aicken ruled that the *Sealed Case* decision had not been informed by arguments from those affected by the surveillance and was wrong.[160]

The government succeeded on appeal, on the grounds that the plaintiffs lacked standing to raise the constitutionality issue. (The plaintiffs had settled all claims in the action except for the claim for declaratory relief.) This meant that it did not have to address the constitutionality issue.[161] However, the district court's reasoning on the constitutional issue has failed to commend itself to subsequent courts.[162]

National Security Letters

In 2004 and 2005, two district courts held that the legislation governing national security letters was flawed, but not because of Fourth Amendment difficulties. The problem lay in provisions precluding the recipient from disclosing receipt of a "request" to produce. One court held that the legislation was unconstitutional on two grounds: it violated the First Amendment, and the lack of provision for judicial review violated the constitutionally prescribed separation of powers.[163] The other based its decisions solely on First Amendment grounds.[164] The New York District Court held further that section 2709(c) could not be severed from the rest of section 2709. There was therefore no authority for the issuing of NSLs. Before the hearing of government appeals, Congress amended the legislation to remove the blanket ban on disclosure and to provide a rudimentary form of judicial review of nondisclosure orders. In light of this, the court of appeals remanded the case to the district court for reconsideration.[165] While the case was pending, the government withdrew the NSLs, which meant that the only issue before the court related to the validity of the nondisclosure requirement. The district court held that the amendments were not sufficient to save section 2709(c) and that if section 2709(c) could not be saved, the rest of the section had to fall with it.[166] The court of appeals substantially agreed with the district court but concluded that sections 2709(c) and 3511(b) (the judicial review section) could be construed so as to save them from unconstitutionality. So construed, the legislation did not violate the Constitution, nor did partial invalidation of the two sections

affect the validity of the remainder of section 2709.[167] The court of appeals remanded the matter for further consideration. In the subsequent litigation, the district court found that the government (which was required to initiate a judicial review application) had made out its case.[168]

The Terrorist Surveillance Program

Revelations about the existence of the Terrorist Surveillance Program provoked a mass of litigation. Despite the general consensus that the TSP was unconstitutional, plaintiffs rarely succeeded, falling victim to a variety of legal hurdles and, ultimately, to legislation aimed at defeating their claims. A challenge to the legality of the TSP by the ACLU and other plaintiffs who claimed to have been injured by the program met with initial procedural and substantive success,[169] but on appeal, the circuit court reversed on procedural grounds.[170] To succeed, the plaintiffs had to be in a position to prove they had standing to sue. The majority held that it was not enough to assert that fears of surveillance meant that the plaintiffs' capacity to perform their various duties was impaired and complicated. They had to prove that the fears were justified, and this would require proof that their communications had been intercepted. Discovery would not assist: the information they needed would constitute a state secret, and state secrets are immune from discovery.

Judge Gibbons dissented, concluding that the plaintiffs had demonstrated harm. The existence of the TSP (which had been acknowledged by the president) meant that the plaintiff's professional obligations precluded them from doing things they otherwise would have done. It also meant that in order for the plaintiffs to perform their professional duties, they would have to use far less convenient means of communication with their clients. This problem would not arise if surveillance were to take place under FISA. In that situation, their professional communications would be protected, so they could freely communicate with their clients, knowing that these communications would be privileged. The Supreme Court denied certiorari.[171]

A claim by the Al-Haramain Islamic Foundation was more successful. Unlike the ACLU, the foundation knew that it had been the victim of warrantless surveillance, having accidentally been shown a document evidencing this, but the court of appeals held that the state secrets doctrine would nonetheless defeat its claim insofar as it was grounded on violation of constitutional rights. It held, however, that a claim for relief under FISA might be capable of being sustained.[172] On remand and after considerable interlocutory skirmishing, the district court held that the state secrets doctrine did not apply to FISA claims, and the plaintiff's claim was made out. But the court of appeals reversed an award of damages and costs against the United States, finding that

the relevant FISA provision (50 USC § 1810) did not constitute a waiver of sovereign immunity in relation to claims for damages.[173]

A large number of cases involved challenges by customers to the cooperation of electronic communications providers.[174] Plaintiffs had some procedural successes. In *Hepting v AT&T*,[175] the district court dismissed motions for summary judgment based on state secrets privilege, lack of standing, and absolute and implied immunity. The plaintiffs' status as customers in contractual relations with the companies satisfied the standing requirement. Given what was known about the TSP, it was not clear that the case would turn on matters that constituted state secrets. For these reasons, summary dismissal was inappropriate. It doubted whether common-law immunity survived FISA, and it also concluded that if the plaintiffs' allegations were proved, the factual basis for reliance on the immunities would be unavailable. Following *Hepting*, the Judicial Panel on Multidistrict Litigation made an order that all cases arising from the NSA's alleged wiretapping be transferred to the Northern District of California and consolidated before Judge Vaughn Walker, who subsequently made orders consolidating the cases against the telecommunications companies, where they were handled under the name *In re National Security Agency Telecommunications Records Litigation*.

A further body of litigation related to attempts by state officials in Maine, New Jersey, Connecticut, Vermont, and Missouri to investigate the role of telephone companies in the TPS. Predictably, these activities provoked the telephone companies and the US government to sue, claiming that the states lacked the relevant powers. These proceedings were also consolidated and transferred to the Northern District of California, where the district court denied the government's motions to dismiss.[176]

At this point, the litigation was complicated by the 2008 passage of the FISA Amendments Act (FISAAA). Section 803 of the FISAAA effectively precluded action by the states in relation to electronic communication service providers' "alleged assistance to an element of the intelligence community," and it applied both prospectively and in relation to pending proceedings. On the basis of this provision, the United States moved for summary judgment in the six telecommunications cases. Arguing that the legislation represented an impermissible encroachment on state powers, the states resisted summary judgment, on the basis that some aspects of their inquiries fell outside the section. The district court disagreed, concluding that the legislation did not commandeer the participation of state officials in a federal scheme: it prohibited their participation. The court stated, "Because intelligence activities in furtherance of national security goals are primarily the province of the federal government, Congressional action preempting state activities in this context is especially uncontroversial from the standpoint of federalism."[177]

The legislation also purportedly barred the existing private suits against the communication companies. This led to a further application from the US government and the telecommunications companies for dismissal of the dozens of cases in which the companies had been sued. The plaintiffs challenged the constitutionality of the legislation on the grounds of separation of powers, arguing that it involved congressional usurpation of the judicial role, in that it made the political branches ultimate arbiters of the requirements of the First and Fourth Amendments, impermissibly required the judiciary to decide pending cases in a particular way, and violated the nondelegation principle. The court rejected these arguments.

Constitutional arguments based on the Fifth, First, and Fourth Amendments failed. Creating new immunities does not violate the right to due process. Nor did the special secrecy provisions: there was considerable authority to support the use of ex parte in camera procedures in cases having national security implications. First Amendment rights were not at stake: cases suggesting that there is a First Amendment presumptive right of access to criminal trials are inapplicable in relation to trials involving classified information, and the procedures prescribed by section 802 sufficed to ensure that it did not offend the Constitution.

Following the legislation, but before these judgments, most of the 150 plaintiffs in one of the multidistrict litigation cases, *Anderson v Verizon*, commenced a new case, *McMurray v Verizon*.[178] The District Court of the Northern District of California also dismissed this case. The jurisdictional prerequisites for an action based on the takings clause had not been established, and in any case, no property had been taken: "no property right vests in a cause of action until a final, unreviewable judgment is obtained." Nor did the legislation fall foul of separation of powers or the Fifth Amendment due process clause.[179]

These judgments did not dispose of cases in which the US government and its officials had been sued. One of these had been filed by plaintiffs in *Hepting v AT&T*, which had been remanded by the Ninth Circuit for reconsideration in light of the legislation. Apparently in response to recognition of the hopelessness of their case against AT&T, four of the plaintiffs had filed a fresh claim, this time against the NSA. In January 2010, the district court granted a government motion for summary judgment in this and another NSA case. It found that the plaintiffs lacked standing. In the earlier *Hepting* case, the plaintiffs had standing by virtue of their injury and their contractual relations with AT&T. In the actions against NSA, the plaintiffs were seeking redress for alleged government misfeasance. The parties lacked a sufficient personal stake in the subject matter of the litigation. That they used telecommunications and were broadband Internet subscribers did not distinguish them from Americans in general, since the vast majority of US households had such connec-

tions. The court advised that standing was to be approached with particular care when constitutional issues were at stake, especially when

> the constitutional issues at stake in the litigation seek judicial involvement in the affairs of the executive branch and national security concerns appear to undergird the challenged actions. In such cases, only plaintiffs with strong and persuasive claims to Article III standing may proceed.[180]

Amnesty International, civil liberties organisations, media organisations, lawyers, and scholars also challenged section 702 of FISAAA as facially unconstitutional. In the district court, the government succeeded on an application for summary judgment, based on the plaintiffs' lack of standing.[181] The plaintiffs' appeal succeeded, and a motion to have the matter heard en banc failed, by majority.[182] The court of appeals distinguished *American Civil Liberties Union v National Security Agency*, finding that the FISAAA authorised much more than the TSP. *ACLU* was not binding (it applied to a different circuit) and was based on a questionable reading of Supreme Court authority. The Supreme Court disagreed. By majority (five Republican appointees against four Democrat appointees), the Court found that the plaintiffs lacked standing. Threatened injury could ground standing only if it was "certainly impending." There was no evidence that the plaintiffs' communications were being intercepted, nor was there reason to believe that interception was impending, and even if interception were to occur there was no reason to believe that it would be pursuant to § 1881a. Expenses incurred for the purposes of avoiding interception cannot ground standing when the interception has not been shown to be certainly impending, nor when there was a similar incentive to take the precautions under pre-existing legislation. The minority concluded that the plaintiffs' fears were well-founded, and past government practices lent them added credibility. The court had not always insisted that harm be "certainly impending," and applied rigorously, the requirement would be unreasonable. The constitutional standing requirement was closer to a "reasonable" or "high" probability of harm.[183] But even if the plaintiffs had won on the standing issue, their victory might have be Pyrrhic: in rejecting a defendants' Circuit Court application for an en banc hearing, Judge Lynch warned, "[T]here are strong grounds arguments against the plaintiffs' position on the merits."[184]

Stops and Searches

Drawing on nonterrorism precedents, courts have also upheld the use of general and "random" stops and searches at airports, subway stations, and ferry terminals as a counterterror measure, concluding that the relevant programs

serve a "special need" and are proportionate, given privacy expectations, the fact that the person could avoid being searched by opting not to use the relevant form of transport, the brevity of the searches, and the preventive and deterrent functions served by such searches.[185] In determining whether the searches serve the legitimate government purpose, considerable deference is given to the government's assessment, and the fact that random searches are less likely to be effective than general searches is immaterial, since random searches also involve less intrusion on privacy interests.[186]

United Kingdom

The only terrorism-related challenge to UK surveillance law involved the stop and search powers under the Regulation of Investigatory Powers Act 2000 (RIPA).[187] A demonstrator and a journalist who were stopped and detained near an "arms fair" challenged the legality of the searches, arguing that the searches were not authorised by the act, that the powers had not been exercised for the purposes of the act, and that the authorisations and the searches were contrary to Articles 5, 8, 9, 10, and 11 of the ECHR. Their argument failed at first instance,[188] in the court of appeal,[189] and before the House of Lords.[190] Moreover, the 10 judges who considered the case were unanimous in concluding against the applicants, who then appealed to the ECtHR, which unanimously held that their Article 8 (privacy) rights had been impermissibly violated.[191]

The House of Lords had obvious reservations about the power but considered that it had a legitimate purpose, "to ensure that a constable is not deterred from stopping and searching a person whom he does suspect as a potential terrorist by the fear that he could not show reasonable ground for his suspicion."[192] The ECtHR agreed that the searches were within the powers conferred by the legislation, but the court found that the exercise of the powers constituted a breach of Article 8: "[T]he use of the coercive powers conferred by the legislation to require an individual to submit to a detailed search of his person, his clothing and his personal belongings amounts to a clear interference with the right to respect for private life."[193] Such searches could therefore be justified only if they were in accordance with the law, pursued a legitimate aim, and were necessary in a democratic society. Since the exercise of the power was largely unconstrained, the legislation failed this test.

One of the ironies of the case lies in the weight that several of the Law Lords attached to the role of intuition.[194] If, as was accepted, police did indeed have a sixth sense for terrorists, there would be much to be said for giving police an unreviewable power to stop terrorists. But the exercise of the stop and search powers put the "hunch" hypothesis to the test. Between 2001–2

and 2008–9, there were more than 540,000 stops in England and Wales under the power. Only 0.9 percent resulted in arrests, and only 0.05 percent resulted in arrests for terrorism offences. None resulted in a conviction for a terrorism offence.[195]

In a challenge to the adequacy of the protections afforded by RIPA to people who claimed to be victims of unlawful surveillance, the ECtHR held that the procedures satisfied the requirements of the ECHR. That the procedures provided for closed hearings by the Investigatory Powers Tribunal was not inconsistent with the convention: it was a proportionate measure, given countervailing security interests.[196]

New Zealand

New Zealand's only "terrorism" prosecutions were prosecuted not as terrorism offences but as firearms and criminal organisation offences. Among the issues to which they gave rise was the question of whether the fruits of covert video surveillance evidence were admissible. The High Court ruled that the evidence was improperly obtained but admissible. The court of appeal ruled that video surveillance could be justified as an extended use of the powers conferred by search warrants.[197] The Supreme Court disagreed: given the relevant legislation, search warrants could not authorise video recording, and the warrants had not purported to authorise it. Nor did the police have any other authority to enter onto the land where they had installed the cameras. Moreover, the Bill of Rights Act prohibited unreasonable searches; the term *search* (in this context) extended to surveillance; and in the absence of authorisation, surveillance was, in the circumstances, unreasonable.

While the Supreme Court had no doubt as to the illegality of the surveillance, it was not unsympathetic to the police. Justice Blanchard recognized that the legal position may not have been altogether clear, but he considered that given the uncertainty, the police should have sought legal advice (but didn't). Blanchard did recognise that the police were caught in a bind.

> They lacked any ability to obtain a warrant for video surveillance because the law did not provide for it, and understandably believed that they could not approach landowners for consent to enter lest the participants in the camps be alerted, and that in person surveillance could endanger members of the police when live rounds were being fired.[198]

In exercising its discretion under section 30 of the Evidence Act 2006 in relation to whether the surveillance evidence might be admitted, the Supreme Court concluded (3–1) that the balance favoured admission in the cases of

those charged with serious "criminal organisation" offences but not in the case of those charged only with firearms offences.

In Short

Despite constitutional and quasi-constitutional protections from search and seizure and from invasion of privacy, courts have done little to interfere with government surveillance. The decision in *Gillan v the United Kingdom* is the only authoritative post-9/11 decision to have found surveillance legislation incompatible with Fourth Amendment or privacy rights. In relation to surveillance, courts seem to share some of the nervousness that underpinned the USA Patriot Act, although they have also expressed some of the concerns of its critics. The English courts' decisions in the *Gillan* litigation and the ECtHR's decision in *Kennedy v United Kingdom* display similar deference, which contrasts with a much more assertive stance in other areas of counterterror law. But the deference is not surprising. Privacy carries less weight than freedom from detention.

US courts have been slightly less deferential in relation to executive decisions. In cases challenging the validity of aspects of the TSP, cases that turned on substance resulted in defeats for the government, whereas cases turning on procedure almost invariably went in favour of the government. Most of the cases turned on procedure, and Addington seems to have underestimated the degree to which the law can frustrate not only authoritarians but civil libertarians. New Zealand courts were a little more resistant to executive interests, but the Supreme Court's ruling did not preclude the use of the offending evidence in the cases where the stakes were highest.

Public Opinion: Restraint or Invitation to Opportunism?

Poll data should always be treated with caution, and there are particular reasons for being cautious about polls relating to surveillance. Haggerty and Gazso have argued that people who are particularly concerned about privacy are probably less likely to cooperate with pollsters and that, as a result, poll data may understate privacy concerns, especially where response rates are low.[199] Unfortunately, they do not provide evidence as to the extent of the problem, and reports on polls rarely include evidence of nonresponse rates.

An alternative problem emerges from a finding by Fletcher to the effect that responses to questions about surveillance are subject to assumptions about the conditions for their exercise. "Elites" are relatively supportive of surveillance, but this seems to be largely because their answers are given in the knowledge that powers are subject to judicial supervision.[200] This high-

lights an inescapable problem: the fact that answers depend on how respondents understand both the question and their answer. Interpreting poll data involves a degree of guesswork.

Nonetheless, post-9/11 polls suggest that the public was somewhat ambivalent towards government surveillance as a counterterrorist strategy and that post-9/11 legislation cannot easily be explained as a response (whether principled or opportunistic) to public receptivity to "tougher" surveillance laws. Polls conducted immediately following the attacks suggested that attitudes towards surveillance varied strongly with the question. Only a quarter of respondents favoured the government being allowed to monitor their personal phone calls and e-mails. Polls relating to surveillance of electronic communications in general typically yielded more disapproval than approval.[201] A poll conducted immediately after 9/11 indicated that a small majority (54 percent) approved of broader government powers to intercept phone calls and that only a bare majority (50 percent, with 5 percent undecided) favoured broader powers to intercept e-mail communications. Far more respondents (68 percent) approved a power to stop people "who fitted the profile of suspected terrorists." A poll conducted a week later yielded similar results. Evidence of ambivalence comes from a contemporaneous Harris poll: more than 70 percent of respondents reported high or moderate concern that increased powers would be associated with increased profiling, the interception of the communications of innocent people, and surveillance of nonviolent government critics; and two-thirds were worried that new powers would be used to investigate nonterrorism crimes.[202] Public concerns about the threat of terrorism do not seem to have been translated into sizeable support for stronger surveillance powers.

In subsequent Harris polls, between 70 and 80 percent of respondents have expressed continuing high or moderate concern about the adequacy of legislative, judicial, and executive supervision of surveillance programs and about the targeting of legitimate political and social groups. Two of these polls also found that 57 percent of respondents thought that law enforcement agencies were using their expanded powers in a proper way.[203]

Polls relating to the Patriot Act suggest that its surveillance provisions commanded majority support, coupled with opposition from a sizeable minority. In polls between 2003 and 2006, bare majorities considered that the act was a "good thing" for America; about a third considered it a "bad thing," and about a tenth volunteered that it was a mixture. Of those who had an opinion, most believed that the surveillance provisions of the act had helped prevent terrorist attacks in the United States, but 41 percent in 2005 and 33 percent in 2006 thought that it had not. Asked whether the provisions should be renewed, most respondents (57 percent) thought they should, but

31 percent opposed renewal. A differently worded question, which included minor change and major change as options, found that only 13 percent favoured no changes and that 50 percent favoured minor changes. Consistent with this is a 2005 poll suggesting that some surveillance provisions commanded far more support than others. There was a very high level of support for allowing the use of foreign intelligence information in domestic crime investigations (81 percent), majority support for government use of communications data (69 percent) and warrants for person-based phone tapping (62 percent), bare majority support for the business records regime insofar as it applied to libraries (53 percent), and opposition to warrantless access to bank records (43 percent support) and sneak and peek search warrants (23 percent support).[204]

In polls conducted following revelations of the TSP surveillance, opinion was evenly divided on the warrantless surveillance of "Americans suspected of terrorist ties," although differently worded questions yielded slightly different approval/disapproval distributions. Slight majorities doubted President Bush's authority to authorise the TSP. A majority thought that communication monitoring was very effective (15 percent) or somewhat effective (48 percent), and a majority were not at all concerned (43 percent) or not very concerned (22 percent) that their own communications might be monitored. Consistent with this lack of concern is a February 2006 finding that only 8 percent of poll respondents thought it likely and 13 percent thought it somewhat likely that their phone conversations had ever been wiretapped; in May 2006, the figures were 9 and 17 percent. Majorities were very concerned (29 percent) or somewhat concerned (33 percent) about losing civil liberties as a result of the administration's counterterrorism measures, but there was slightly less concern about the capacity of such measures to violate "people's privacy." Only 10 percent of poll respondents had a great deal of confidence in the government's capacity to identify correctly those whose phones should be tapped; 46 percent had a fair amount of confidence, and 42 percent had very little or no confidence.[205]

The impact of the TSP revelations on aggregate public opinion seems unclear. A Harris poll provided no evidence to suggest a decline in support for surveillance between June 2005 and February 2006 (indeed, the trend was in the opposite direction, albeit nonsignificantly). While majorities no longer favoured expanded powers to intercept communications, 82 percent favoured expanded undercover penetration of suspected groups; 67 percent, expanded camera surveillance; 64 percent, adoption of a national identification system; and 60 percent, monitoring of Internet discussions.[206] Other series of polls suggest continuing support for monitoring of those regarded by the govern-

ment as suspicious, but they suggest widespread opposition to sharing data on communications or purchasing patterns with the government.[207]

Poll data relating to surveillance in the other countries is sparse, which probably reflects the limited salience of surveillance issues. In a 2004 UK survey, 69 percent approved police powers to stop and search anyone at any time.[208] Surveillance in public places commands widespread approval (generally more than 80 percent), except when it involves eavesdropping using high-powered microphones (commanding 9 percent approval).[209]

Fletcher's 1989 survey suggested that Canadians were particularly likely to say that the Canadian Security Intelligence Service should have wiretapping powers when the target was "suspected terrorists" rather than mere suspected subversives, support being high among the general public (66 percent) and even higher among a heterogeneous elite sample (81 percent).[210] There appears to be little recent poll data on the subject, apart from a tangentially relevant 2005 poll indicating that 72 percent of Canadians supported video cameras in public places.[211]

A 2007 Australian survey indicated that 39 percent of respondents thought police should definitely have the right to tap the phones of those they suspected of being terrorists, and 38 percent thought they should probably have the right. Only 8 percent thought they should definitely not have the right. There was, however, much less support for a police power to stop and search suspected terrorists in the street: 24 percent thought they should definitely have the right, and 31 percent thought that they should probably have it. Twenty percent thought they should definitely not have the right.[212]

The poll data suggests that there are few votes to be won by advocating stricter surveillance. The public tends to support surveillance of suspected terrorists and seems supportive of video cameras in public places, but it tends to oppose more-intrusive forms of surveillance, indiscriminately applied. At least in the United States, support for some forms of surveillance coexists with scepticism as to whether governments will target surveillance with acceptable precision. Willingness to sacrifice civil liberties does not extend to tolerating a significant risk of one's own private conversations being monitored. In this respect, there is little support for explanations of this area of law in terms of reluctant politicians responding to popular demands for repressive measures. Indeed, the political response is more consistent with public opinion constituting a constraint on repressive measures. Legislators have acted as if they were aware of this: "nongovernment" legislators seem to have never advocated and sometimes resisted greater surveillance powers than those being sought by the government. Taking a civil libertarian stance may sometimes be electorally expedient.

Partisanship and Surveillance

There are several guides to the role of political beliefs as a determinant of stances on surveillance law. One comes from roll call votes. These generally indicate that support for extended surveillance powers tends to come more from Republicans than from Democrats. The few members of Congress to vote against the Patriot Act were all Democrats, and party affiliation has been related to subsequent measures including extending sunset periods and the 2007 and 2008 amendments to FISA. The May 2011 measures involved a degree of leakage. In the House, the yeas included 196 Republicans and 54 Democrats; the nays, 31 Republicans and 122 Democrats. In the Senate, where support for extension was greater, the majority included 41 Republicans, 30 Democrats, and an Independent. The nays included 18 Democrats, 4 Republicans, and an Independent. These latter figures suggest that the impact of political dispositions is largely independent of whether the party supporting the measures is in government—at least in the United States.

Elsewhere, post-9/11 measures have impinged only marginally on liberty and privacy issues, but in Australia, where interception continues to be controversial, partisan positions tend to be related to the parties' rank along a right-left continuum, blurred slightly by the exigencies of being in power. It was, after all, a Labor government that tried to legislate to give ASIO the power to seek warrants for roving interception.

Congressional voting patterns are reflected in the correlates of public attitudes towards surveillance. The reported results for a *CBS News* poll tapping attitudes towards "Bush administration practices" reported an extremely strong relationship between party identification and beliefs about the legitimacy of the TSP. Eighty-three percent of Republicans, 42 percent of Independents, and 33 percent of Democrats approved, but that is what one might expect given the express reference to the Bush administration. A question asking whether the president should have the power to authorise the NSA to monitor communications yielded a similar (but slightly weaker) relationship: 79 percent of Republicans, 49 percent of Independents, and 35 percent of Democrats agreed.[213] Party bore a similar relationship to whether the NSA's analysis of phone call data constituted a necessary tool or went too far in invading privacy.[214] One (unlikely) explanation for this might be that Republicans and Democrats are, politically, two quite different species. Another is that in its selection of professed attitudes, the public relies heavily on cues given by spokespeople with whom they identify. Questions not framed in terms of the Bush administration's actions might have elicited a less-partisan set of responses.

An analysis of the effects of party identification after controls for perceived terrorism threat, authoritarianism (as measured by attitudes towards child rearing), ideology, and demographic variables indicated that party exerted an independent

influence on support for warrantless wiretapping but that authoritarianism, ideology, and threat perceptions were also associated with support. It further indicated that among those who were worried about the personal threat posed by terrorism, authoritarianism was unrelated to support for wiretapping. (It did not examine whether this was the case for other predispositional measures.)[215]

In a 2007 Australian poll, the relationship between voting intention and attitudes towards surveillance seems to be weaker. Among Liberal (conservative) voters, 53 percent definitely believed that police should have the power to tap suspected terrorists' phones, and 34 percent thought that they should probably have the power. Among their National (rural) allies, the figures were 45 and 35 percent. There was less support from Labor voters (31 and 41 percent) and Greens (24 and 35 percent). The positions of supporters of other parties were consistent with their stance on the Australian left-right continuum, but only weakly. On the power to stop and search terrorism suspects in the street, Liberals were most supportive (33 percent), followed closely by Nationals (28 percent) and Labor voters (19 percent). Greens were considerably less supportive (10 percent).[216]Again, preferences of voters for other parties corresponded to their general dispositions. The differences are less pronounced than in the United States, probably because government surveillance had not been a major political issue.

Conclusions

While the USA Patriot Act has come to symbolise the evils of counterterrorism law, it is arguably a distraction. Critics of the act (including some of those who nonetheless voted for it) warned that its expanded surveillance powers were unconstitutional. Drawing on a supportive history, they feared abuses. However, even after the passage of the act, the government's powers in relation to domestic terrorism generally fell short of those of the other governments, and its powers in relation to international terrorism were generally more circumscribed. Moreover, later abuses involved not the misuse of powers but acting outside them, and courts have generally upheld the constitutionality of the Patriot Act provisions (except insofar as they purported to permit inadequately reviewable gag orders). Elsewhere, surveillance law has proved less controversial, although the history of the UK stop and search powers highlights both the potential for abuse and the fact that if vagueness were to doom laws to unconstitutionality, bills of rights would be the first casualty. Poll data suggest that the issue is one capable of provoking strong feelings that are based on limited knowledge. Academic disputes, parliamentary debates, and roll calls suggest that being relatively well informed does not resolve those differences. It is therefore not surprising that there is evidence to suggest that stances on the issue are partly bound up with political dispositions.