Leashing the Internet Watchdog: Legislative Restraints on Electronic Surveillance in the U.S. and U.K.

John P. Heekin

Available at: https://works.bepress.com/john_heekin/1/
Leashing the Internet Watchdog: Legislative Restraints on Electronic Surveillance
in the U.S. and U.K.
John P. Heekin

As a general principle, technology is neutral with regard to privacy. It is the rules
governing the use of technology that matter. [...] Within the proper set of rules, we can protect
privacy while using technology to modernize government systems for domestic defense.†

Some will say that the innocent have nothing to fear by disclosure. It is only the wicked
and villains who should worry. But that is not true. The right to privacy long predates any
human rights legislation. [...] The more intrusive and secretive the powers, the more pernicious
the abuse.‡

I. Introduction

As the capacity and availability of electronic and wireless communications has
dramatically expanded over the last twenty years, intelligence and security services worldwide
have raced to develop the means to keep pace with the changing needs of national and domestic
security. Technology has facilitated global connectivity in ways previously unimaginable, and
electronic transmissions – from cellular telephones, to email and instant messaging – have
become a ubiquitous medium for personal and business communications worldwide.

Unfortunately, improvements to international connectivity have been accompanied by new
threats to global security,¹ in turn leading governments to implement regulatory mechanisms to
monitor the endless streams of electronic data racing across borders around the world.

This article examines the legislative approaches undertaken by the United States and the
United Kingdom to regulate the surveillance and interception of electronic communications,
while recognizing that a balance must be struck between the preservation of national security and
the protection of individual privacy interests. The question need not be one of privacy or

---

† Shane Ham and Robert D. Atkinson, Using Technology to Detect and Prevent Terrorism, Progressive Policy
‡ Grahame Danby, “Communications Data: Access and Retention,” House of Commons Library Research Paper
02/63 at 38 (21 Nov. 2002) (quoting statement made by Lord Phillips of Sudbury in the House of Lords debate from
27 November 2001.).
security, because the effective planning, uniform implementation, and thorough oversight of comprehensive safeguard measures by legislatures can harness the utility of technology to accomplish both. In fact, data mining programs designed and implemented with close collaboration between intelligence services and legislative bodies would be able to fulfill the need for timely, effective and accurate intelligence information extracted from massive quantities of electronic data, while ensuring adequate and appropriate safeguards are in place to protect against government abuse.  

Given the particularly ominous possibilities for the interception of private electronic communications by the government, it is not surprising that the disclosure in 2000 of a data mining program operated by the U.S. Federal Bureau of Investigation, nicknamed “Carnivore,” caused significant alarm among the public and internet service providers. News of the program led to formal inquiries by both Chambers of the U.S. Congress, as well as an independent technical review of the system and its safeguards. Though the power to initiate formal hearings and require agencies to come before Congress is a powerful tool of effective oversight, this article will focus primarily on the statutory provisions enacted by the legislature to control the means, manner and extent of electronic surveillance.

Part II will provide a brief, non-technical overview of data mining practices employed by systems like Carnivore, as well as a cursory look at the disclosure and investigation of the FBI’s controversial program. Next, Part III will explore the privacy norms developed in the U.S. and U.K., noting the differences in structure, but the similarities in application between the Fourth Amendment and Article 8 of the European Convention on Human Rights. Part IV will shift focus to the parliamentary power to conduct oversight through the passage of legislation, outlining the frameworks designed to regulate the implementation of electronic surveillance by
intelligence and security services. Lastly, Part V will conclude with present examples of
electronic surveillance in action, noting a recent shift in both the U.S. and U.K. toward more
intrusive measures to monitor and intercept electronic communications.

II. Data Mining Technologies

Introduction

Data mining refers to the process of using automated analysis technologies that apply an
algorithm with manually configured collection restrictions to a large compilation of datasets in
order to connect independent but related pieces of information to develop useful patterns that
may be exploited for business, scientific or domestic security purposes. The primary value of
data mining technologies to intelligence and security services is the ability to sift through
volumes of datasets for a more accurate and timely analysis than could otherwise have been
obtained through traditional investigative measures. In turn, more accurate and timely analysis
offers the increased likelihood that intercepted information may be transmitted to the appropriate
law enforcement agencies, with interdiction before the conspiracy turns reality.

The core function of data mining is two-fold: to derive information from numerous
sources that was previously unknown; and to develop that information into a product that is
potentially useful to its recipient. As for the former, the program can help to answer a question
that has not yet been raised by identifying patterns or tangential relationships that are not
otherwise obvious, but which exist in the data itself. The data mining program may then
organize the information as a simple summary of the findings, a descriptive model of patterns, or
a predictive analysis of the relationships between various data points, depending on the needs of
the investigator. The usefulness of the data derived is wholly dependent upon the collection
restraints included in the program’s configuration, which subject the processed information to an “interestingness” test to measure the pattern’s value according to the information sought.¹⁰

Process Overview

Data mining consists of three stages – pre-processing, descriptive and predictive modeling, and post-processing – each of which play a vital role in the value of the final product. In pre-processing, the operator must first identify desired outcomes for the program to use in evaluating the relevance of information, after which the data is collected, selected and stored in a single set for further processing. A subsequent process then “cleanses” the data by eliminating redundant and otherwise useless pieces before standardizing the set for the modeling stage.¹¹

At the middle stage, the data is actually “mined” by applying pre-defined algorithms to extract, identify and reveal unknown relationships within the dataset that emerge as descriptive or predictive patterns. In developing the patterns, the program may be instructed to apply either a “top-down” or a “bottom-up” approach, where the former uses a specific hypothesis that is sought to be validated, and the latter extracts patterns on which subsequent hypotheses may be based.¹²

In post-processing, the patterns and relationships must be interpreted and analyzed according to their usefulness within the defined scope of the operation.¹³ Although the timeliness of automated analysis is of great value to data mining operators, particularly in the domestic security context, the importance of human review of the patterns and results cannot be overlooked, and is a necessary component of oversight to ensure the minimization of false-positives. Furthermore, given the likely absence of an articulated suspicion of an individual prior to his identification by the data mining program, there is substantial U.S. constitutional weight
behind the argument that such programs must be used in only an investigative capacity, and not an evidentiary role.\textsuperscript{14}

\textit{Investigation and Disclosure of Carnivore}

The U.S. Federal Bureau of Investigation (FBI) developed Carnivore\textsuperscript{15} as a software-based investigative tool designed to filter and record pre-defined data packets traveling through an Internet Service Provider’s (ISP) ethernet connection.\textsuperscript{16} The system was created to be implemented in judicially-authorized electronic surveillance operations when alternative programs were either unavailable or insufficient to meet the needs of investigators while adhering to stringent safeguard protocols demanded by the court.\textsuperscript{17} Although the Carnivore system was deployed within a framework of procedural safeguards, both judicial and programmatic,\textsuperscript{18} the FBI’s ability to intercept electronic communications and monitor Internet usage nonetheless sparked widespread concern from the general public and ISPs.\textsuperscript{19} In the face of competing interests between law enforcement, seeking continued access to information pertinent to criminal and national security investigations, and the general public, concerned with the preservation of privacy in modern communications, Congress called for hearings on the issue.

In addition to the passage of legislation establishing guidelines for government conduct, effective oversight requires parliamentary bodies to conduct investigations into intelligence and security services’ compliance with those mandates.\textsuperscript{20} Fulfilling this role, in July and September 2000, separate hearings were held before the House and Senate Committees on the Judiciary to address concerns raised by the FBI’s use of Carnivore.\textsuperscript{21} Both hearings sought to examine the Fourth Amendment implications of electronic surveillance over Internet communications, and heard testimony from numerous sources, including civil liberties advocates and representatives of the FBI and Department of Justice.\textsuperscript{22} Although both sides exchanged volleys in their
respective testimony, little came from the hearings except a realization that the advent of modern communications technology presented a quagmire for both law enforcement interests and Fourth Amendment privacy concerns.23

Perhaps the only substantive result of the congressional hearings was the FBI’s abandonment of the Carnivore program as its principal mechanism to conduct electronic surveillance of Internet communications, opting instead to use commercially-available software to fulfill such needs.24 The demise of Carnivore may only be a Pyrrhic victory for civil liberties advocates, however, given the findings that its safeguards were superior to commercially-available software programs, and thus less likely to acquire information beyond the scope of a court order than its peers.25 Nonetheless, it is clear that technological advancements have had and will continue to have an impact on privacy, and the government recognition of the person’s privacy interest in the face of those developments will be explored in the following section.

III. Privacy Norms of the U.S. and U.K.

Government-operated electronic surveillance, such as the Carnivore program, has serious implications for individual privacy in a world increasingly reliant upon electronic and wireless communications. Legislative and judicial recognition of privacy interests are particularly important assurances to the democratic electorate against the possibility of abusive or discretionary infringements of citizens’ private lives by government agencies. On the other hand, approving of limited encroachments for the preservation of national security and public well-being is necessary to ensure the safety of the populace against threats, both external and internal. With appropriate restraints, the question need not be one of privacy or security, as both may be achieved in equal measure.
The U.S. Constitution is the principal authorizing and limiting source for government conduct, and though a right to privacy is not explicitly included within its provisions, the Fourth Amendment is the most direct and oft-cited expression of such an interest.\textsuperscript{26} By contrast, until its incorporation of the European Convention on Human Rights (ECHR) in 1998, the United Kingdom had not fully recognized a general privacy interest of the individual, though various committee reports had reflected upon the necessity of observing such a right.\textsuperscript{27} Although the structures of the two provisions differ, the core concept embraced is largely the same – protection of the individual’s private affairs against unwarranted government intrusion.\textsuperscript{28}

\textit{Evolution of the Reasonable Expectation of Privacy in the U.S.}

In the United States, the interpretation and application of the laws is left to the courts, and extensive litigation has been devoted to the reasonableness of government conduct within the framework of the Fourth Amendment. The Supreme Court decision in \textit{Katz v. United States} marked the shift in U.S. jurisprudence from a property-based recognition of privacy rights\textsuperscript{29} to the observation that the Fourth Amendment was intended to protect people, not places.\textsuperscript{30} In addition to recognizing the personal nature of the interests protected, the holding emphasized the importance of a search warrant issued by an impartial judicial officer to strike a balance between individual privacy and the needs of law enforcement.\textsuperscript{31} The Court specifically noted, however, that the case did not address the sufficiency of alternative safeguards implemented in the absence of prior judicial approval where the investigation pertained to national security.\textsuperscript{32}

\textit{Katz} is best-known for Justice Harlan’s concurring opinion articulating the test for an individual’s Fourth Amendment privacy interest in the face of a government search.\textsuperscript{33} The Fourth Amendment protections were triggered where an individual demonstrated a subjective expectation of privacy, and that expectation was reasonable within the view of society.\textsuperscript{34}
Although the subjective element of Harlan’s evaluation has been criticized for its susceptibility to minimization by external forces, the value of the objective reasonableness determination has persisted.

The development of more advanced surveillance technologies has impacted the reasonable expectation of privacy over the years, but the breakwater determination has remained true to the distinction in *Katz* between the observation of activities knowingly-exposed to the public and those intended to remain private. Subsequent decisions upheld the warrantless utilization of surveillance technologies to monitor the telephone numbers dialed from a residence and to track the movements of an individual travelling along public roads and highways, because in both instances the information obtained was voluntarily and knowingly exposed to the public view. However, the Court has been clear that the guarantees of the Fourth Amendment draw “a firm line at the entrance to the house,” so that the reasonableness of government conduct in such cases would depend upon the acquisition and adherence to a judicially-issued warrant.

With its holding in *Kyllo v. United States*, the Supreme Court ruled against the government’s use of intrusive technology, but with an important caveat that may have opened the door for broader, rather than narrower use of such means without a warrant. While recognizing that advances in technology had eroded aspects of privacy secured by the Fourth Amendment, the Court ultimately concluded that the implementation of devices not in “general public use” to monitor activities within the home was presumptively unreasonable in the absence of a court order. Reading between the lines of the opinion, it appears to revive the “subjective prong” of Justice Harlan’s “reasonable expectation test” from *Katz*, so that the wide availability
of intrusive technology would arguably support its application by law enforcement without requiring a warrant for such use.\textsuperscript{44}

In sum, the Fourth Amendment generally requires the acquisition of a warrant for Government surveillance.\textsuperscript{45} However, where the Government monitors the activities of a person without a warrant, a violation of the Fourth Amendment depends upon a determination of reasonableness – the reasonableness of an individual’s expectation of privacy, and the reasonableness of the police conduct in relation to that expectation. The individual cannot have a reasonable expectation of privacy in information he voluntarily exposes to the public, and such activities may be observed by law enforcement agencies without prior judicial approval so long as they remain entirely within the public view.\textsuperscript{46}

The Fourth Amendment is the platform from which other statutory provisions must be based, as the ultimate test of subsequent legislation is its compatibility with the U.S. Constitution.\textsuperscript{47} Conversely, although the U.K. explicitly incorporated the ECHR into domestic law through the Human Rights Act 1998, the very terms of the statute permit the government to interfere with that privilege so long as it does so “in accordance with the law.”\textsuperscript{48} The question then becomes, exactly what right to privacy is recognized in the United Kingdom?

}\textit{Respect for Private Life and Privacy in the U.K.}\textit{ }

Despite helping to draft the ECHR in 1950, and attempting to abide by its terms since that date, the U.K. did not fully bind itself and its courts to uphold the provisions of the international agreement until the enactment of the Human Rights Act 1998, which came into force in October 2000.\textsuperscript{49} Though seeming to embrace the general right of privacy with its incorporation of the ECHR, the provision in Article 8 is categorized as a “qualified right,” meaning it is subject to interference under select circumstances.\textsuperscript{50} For example, enforcement of
the obligation to respect the individual’s private life is lacking where another Act of Parliament renders compliance impossible. In other instances, the prohibition of government interference is altogether abandoned when such intrusion is authorized by another law, or declared necessary for various interests of the State, such as national security and crime prevention. These qualified exceptions offer a particularly large loophole within which the government may justify the implementation of surveillance measures or other actions performed under the authority of primary legislation.

Similar to the evaluation of a “reasonable expectation” of privacy in the U.S., the scope of an individual’s “private life” under Article 8 has been the subject of numerous lawsuits before the European Court on Human Rights and various tribunals within the United Kingdom. The right has been interpreted broadly to include “such personal privacy as is reasonable in a democratic society, taking into account the rights and freedoms of others.” However, more often than not, the deciding factor in cases alleging violations of Article 8 has been the failure of a public authority to abide by the law or adhere to established protocol when conducting surveillance, rather than the affirmation of an inalienable right to privacy.

Respect for individual private life has been argued to include a right to preserve the confidentiality of various forms of information, such as official records and medical data, as well as a right to be informed when a person is the subject of an investigation. Additionally, the right has been extended to protect the individual from covert video surveillance where it is conducted outside the scope of the law. Meanwhile, respect for the home prevents interference with the entrance to or occupation of a dwelling, as well as the right to the peaceful enjoyment of the residence. Furthermore, the right to respect for a person’s correspondence has been
interpreted to include emails and telephone calls, and protection follows the individual both at home and at his place of employ.\textsuperscript{59}

The case of \textit{Halford v. United Kingdom}, which pertained to the right to privacy in a person’s telephone calls, is of particular interest because it incorporated language similar to \textit{Katz}.\textsuperscript{60} The Chief of Police had implemented secret wiretapping of Halford’s home and work telephones without authorization of the law, and so the covert surveillance violated Article 8 because the phone calls were considered to be part of her “private life” and “correspondence.”\textsuperscript{61} More importantly, however, the court based part of its judgment on the “reasonable expectation of privacy” that she had in the use of those phones, noting that a work phone could still be considered “private” because she had not been warned that her calls were subject to interception.\textsuperscript{62} To follow Justice Harlan’s test from U.S. Fourth Amendment jurisprudence, it could be said that Halford had a subjective expectation that her phone calls were to remain private, given the lack of warning that she may be subjected to monitoring, and that expectation was reasonable in the eyes of society for the same reason.

Thus, though differing in structure, the privacy protections of the U.K. and U.S. appear somewhat similar in application. As noted above, the test for a Fourth Amendment violation is whether the individual had a subjective expectation of privacy that may also be deemed reasonable in the eyes of society.\textsuperscript{63} In the U.K., that same approach could arguably be applied because the existence of a statute authorizing intrusive conduct by a public authority diminishes an individual’s subjective expectation of a right to privacy in such activity, and supports the government claim that no violation of Article 8 has occurred. Alternatively, where no such legislation exists, the personal claim of a violation of the right to private life is strengthened and
the legitimacy of the government action is undermined without additional justification under one of the prescribed State interests.

Judicial decisions in the U.K. and U.S. and their statutory bases – the ECHR and the Fourth Amendment – have impacted subsequent legislation enacted by each country to varying degrees, as will be examined in the following section.

IV. U.S. and U.K. Statutory Oversight of Electronic Surveillance

Typically, parliamentary oversight of the intelligence and security services is split between the primary functions of legislation – the means by which the parliamentary body issues mandates and formulates the operational budget – and investigation – the process of ensuring compliance with national laws and monitoring the conduct of the services. The role of legislation is particularly important because it is the most far-reaching method available to representational bodies to control the conduct of intelligence and security services, as well as the means by which the interests of the democratic electorate may be preserved. Such regulation is vital in relation to invasive measures, like electronic surveillance, which require strict parameters to prevent the abuse of domestic and international privacy norms. This section will focus on the legislative developments leading to the creation of the modern statutory vehicles intended to regulate electronic surveillance in the U.S. and U.K. – the Foreign Intelligence Surveillance Act (FISA), and the Regulation of Investigatory Powers Act (RIPA).

*Development of Legislative Controls on Government-Operated Surveillance*

After the U.S. Supreme Court decision in *Katz*, and following concerns voiced in congressional hearings regarding pervasive warrantless executive branch surveillance, Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act in 1968. The Act was the first piece of legislation requiring the President to obtain a court order prior to
conducting domestic electronic surveillance, and sought to distinguish foreign surveillance from domestic criminal investigations.\textsuperscript{68} In addition to requiring prior judicial approval, the legislation defined the framework through which a court order could be issued for domestic surveillance and established “probable cause” as the legal standard necessary to justify such activity.\textsuperscript{69} Though seeking to curb the power of the executive branch to act without prior judicial approval, Title III’s national security exception was frequently used to justify government surveillance until it was successfully challenged in \textit{United States v. U.S. District Court for the Eastern District of Michigan (“Keith”).}\textsuperscript{70}

In \textit{Keith}, the Supreme Court held that although the President was authorized to conduct operations in the interest of national security, such actions must remain compatible with the warrant requirements of the Fourth Amendment.\textsuperscript{71} Despite the clear judgment by the Court, a number of government scandals related to warrantless surveillance arose in the years following the decision, ultimately prompting Congress to form the Senate Select Committee to Study Government Operations with Respect to Intelligence Activities, chaired by Idaho Senator Frank Church.\textsuperscript{72} The Church Committee, as it has become known, was tasked with investigating alleged intelligence abuses by government agencies, and its final report to Congress concluded that domestic surveillance without a court order was a pervasive threat.\textsuperscript{73} The report found that the national security exception had been frequently employed to circumvent the statutory requirements of Title III,\textsuperscript{74} which signaled a distinct need to fill the gaps left by the Act’s inability to monitor and regulate the acquisition of foreign intelligence information.

Similar to the development of Title III in the U.S. following \textit{Katz}, the creation of a statutory framework for the interception of communications came in the U.K. only after a decision of the European Court of Human Rights noted the lack of such procedures in domestic
law. The case of *Malone v. United Kingdom*, dealt with the wiretap surveillance of a London antique dealer suspected of handling stolen property. It is interesting to note that although the wiretaps were in place under a warrant obtained from the Secretary of State, the surveillance was nonetheless held to be a violation of Malone’s Article 8 right to respect for private life because wiretapping lacked a statutory basis in the U.K., and was, thus, not conducted “in accordance with the law.”

Following the decision in *Malone*, Parliament enacted the first piece of legislation specifically authorizing the implementation of wiretapping in the U.K. – the 1985 Interception of Communications Act (ICA). The ICA established conditions to be met prior to the issuance of a wiretapping warrant, giving a legally-enforceable character to such requirements for the first time, but was largely ineffective to truly regulate electronic wiretapping. Loopholes in the legislation, such as broad provisions for emergency wiretaps, meant the requisite conditions were not always met prior to implementation of surveillance operations, and the lack of effective oversight measures allowed such failures to go unchecked. The ICA, however, remained the primary authority for wiretapping operations until 1997 when another case before the European Court of Human Rights exposed its shortcomings and led to the development of the modern statutory framework for electronic surveillance in the U.K.

*The Foreign Intelligence Surveillance Act of 1978*

Following the exposure of Title III’s shortcomings by the Church Committee, and buttressed by the Supreme Court’s holding in *Keith*, Congress sought to limit the executive branch’s power to conduct warrantless surveillance without impeding the capacity to address legitimate threats to national security. As originally enacted, FISA regulated electronic surveillance conducted within the U.S. by requiring prior judicial approval under most
circumstances for the acquisition of foreign intelligence information \(^{82}\) from a foreign power or its agents. \(^{83}\) Though FISA supplemented Title III’s regulation of electronic surveillance by filling in the gaps left in its coverage, it was designed primarily to address national security interests rather than to facilitate the investigation and prosecution of crime by law enforcement. \(^{84}\)

The statute authorized electronic surveillance to be initiated in three ways: (1) upon certification by the Attorney General; (2) pursuant to the so-called “emergency powers” of the executive branch; or (3) through the acquisition of a warrant from the Foreign Intelligence Surveillance Court (FISC).

Under the first, the President could authorize the implementation of electronic surveillance for up to one year without a court order, so long as the Attorney General certified that it was intended solely for foreign intelligence information, only foreign powers and their agents were targeted, and there was not a “substantial likelihood” that the surveillance would acquire information from a U.S. party. \(^{85}\) This is the only category of surveillance that does not need authorization or approval of a court order, though the second method made a concession for national security interests in the face of exigent circumstances. The exercise of “emergency powers” enabled the Attorney General to authorize electronic surveillance upon the reasonable determination that an emergency situation necessitated the deployment of such measures without first obtaining a court order from the FISC. \(^{86}\) Given the potential for abuse of surveillance authorizations without first having to obtain a warrant, the period for such emergency implementation was short, and the Attorney General was required to inform the FISC of the action and seek approval within 24 hours. \(^{87}\)

Submitting an application to the FISC required the Attorney General to identify the targeted individual as a foreign power or its agent, describe the type of surveillance to be
deployed, and certify that the information was sought for “the purpose” of foreign intelligence. In addition, sufficient detail had to be provided to justify a determination of probable cause that electronic surveillance would most effectively fulfill a legitimate need that could not be achieved by less intrusive means. Such information included the identity of the target, the nature of the information sought, the expected period of deployment, and the kinds of surveillance measures to be used, along with the minimization procedures to be implemented as safeguards against abuse.

The passage of FISA may be viewed as an effective exercise of legislative oversight by Congress, in that it addressed the shortcomings of Title III revealed through the investigations of the Church Committee, and balanced the need for Executive flexibility to protect national security with the privacy interests of U.S. citizens. The statute remained largely unaltered for more than 20 years until Congress passed the USA PATRIOT Act in the wake of the devastating terrorist attacks of September 11, 2001, which amended various sections of the 1978 statute to broaden the scope of permissible government surveillance. Whereas FISA exemplified the role of effective legislative oversight in addressing gaps in an existing framework and responding with appropriate revisions, the PATRIOT Act reflected the danger of legislative acquiescence to Executive Branch pressure and general public panic.

Perhaps the most impactful amendment made by the PATRIOT Act was the broad expansion of executive authority to conduct electronic surveillance by the simple alteration of a single word in FISA, changing the application requirement to a certification that information was sought for the “significant purpose” of foreign intelligence. Prior to the amendment, surveillance was only authorized under FISA if it was conducted for the purpose, i.e., the primary purpose, of acquiring foreign intelligence information. By allowing operations to be
conducted with only the significant purpose of acquiring foreign intelligence information, the
government could turn to FISA for authorization of its domestic surveillance so long as at least a
secondary purpose was to acquire intel regarding national security. A 2002 decision by the
FISC recognized the congressional intent behind the alteration and interpreted the new language
broadly to authorize electronic surveillance under FISA so long as the foreign intelligence
objective passed the “significant purpose” test. Though it may be premature to call the
expansion a step toward the generalized warrant the Fourth Amendment was drafted to guard
against, it certainly broadens the ability of the government to conduct surveillance authorized
under FISA.

Despite the expansive authority granted by the amendments to FISA within the
PATRIOT Act, a 2005 New York Times article revealed an Executive Order signed in 2002
exempting from warrant requirements select surveillance performed by the National Security
Agency (NSA) of international telephone calls and email messages sent from within the U.S.
News of the program prompted criticism of the warrantless surveillance, but, more importantly,
highlighted a grey area in the statutory framework that was not directly addressed by existing
legislation – the interception of communications within the U.S. that were sent outside U.S.
territory. The authority to conduct such operations was ultimately granted through the hasty
passage of the Protect America Act of 2007 (PAA), which allowed the government to conduct
surveillance from within the U.S. of foreign communications for a period of up to one year
without court approval. Though the PAA itself was short-lived, more amendments to FISA
were in the works that encapsulated some of its provisions and expanded the government’s
surveillance power once again.

\textit{FISA Amendments Act of 2008}
Following the expiration of the PAA in early 2008, Congress drafted the FISA Amendments Act (FAA) as the most recent addition to the statutory framework of electronic surveillance regulations. To clarify the circumstances under which the government could engage in covert electronic surveillance, the FAA established that its provisions, along with those of Title III\textsuperscript{104} and statutory regulations pertaining to pen registers and stored communications,\textsuperscript{105} were to be the exclusive means by which lawful surveillance could be initiated within the U.S.\textsuperscript{106} This provision was intended to put to rest the contention that the government had legal authority to act outside the scope of FISA in implementing electronic surveillance, as well as the argument that Congress lacked the constitutional power to regulate such measures.\textsuperscript{107}

In addition to establishing FISA and related statutes as the exclusive means by which the government may conduct electronic and communications intercept operations \textit{within} the U.S., the FAA sought to provide for the surveillance of targets located abroad through a new Title VII of FISA.\textsuperscript{108} The statute authorizes the targeting of individuals reasonably believed to be located outside the U.S., and defines the guidelines to conduct such operations in a lawful manner while ensuring the preservation of privacy interests and civil liberties for U.S. citizens.\textsuperscript{109} Consistent with the original FISA provisions, the stated purpose of the surveillance must be to acquire foreign intelligence information, but procedures to lawfully conduct such operations were slightly altered.

First, the FAA permits the targeting of persons, other than U.S. person, who are reasonably believed to be located outside the U.S. To obtain a court order in such circumstances, the Attorney General must certify that the scope of the surveillance is limited to non-U.S. persons reasonably believed to be located outside the U.S., and appropriate minimization procedures are in place to ensure the operation does not directly or indirectly target a person
known to be in the U.S. or a citizen.\textsuperscript{110} Unlike court order requirements for standard FISA surveillance, the form of communication subject to interception does not need to be specified in the application to the FISC, so long as the target is reasonably believed to be outside the U.S. and is not a U.S. person.\textsuperscript{111} Following approval by the FISC, and upon authorization by the Attorney General and the Director of National Intelligence, surveillance operations under this category may be conducted for up to a year before the court order must be renewed.\textsuperscript{112}

Additionally, the FAA provides for the targeting of U.S. persons reasonably believed to be located abroad either through the interception of communications from within the U.S., or using other surveillance measures outside the U.S.\textsuperscript{113} An application to the FISC must establish that the U.S. person is reasonably believed to be located outside the U.S., and must also present the facts and circumstances necessary to develop probable cause that the target is an agent of a foreign power.\textsuperscript{114} For the domestic interception of communications, a court order issued permits the government to conduct electronic surveillance of the individual so long as the information is acquired from sources within the U.S., i.e., passes through domestic channels.\textsuperscript{115}

On the other hand, the intelligence services are forbidden from targeting U.S. persons outside the country without a FISC warrant under circumstances in which the individual would have a reasonable expectation of privacy.\textsuperscript{116} This is the first such requirement that intelligence services acting outside the U.S. must obtain FISC authorization before surveillance operations may be lawful.\textsuperscript{117} Similar to Justice Stewart’s assertion in \textit{Katz} that the Fourth Amendment protects “people, not places,”\textsuperscript{118} this provision of the FAA recognizes that the Constitution attaches to the individual citizen and its protections are not contingent upon his presence within the U.S.
In addition to measures expanding the government power to implement electronic surveillance, the FAA also included several important oversight provisions to govern the newly-expanded authority. Semi-annually, the Attorney General and Director of National Intelligence are required to assess compliance with targeting and minimization procedures, which must be submitted in a report to the congressional intelligence committees. Additionally, the legislation requires the Attorney General to submit to the congressional intelligence committees all decisions, orders and opinions of the FISC that significantly construct or interpret any portion of the Act within 45 days of the action, along with similar materials from the prior five year period. This measure is particularly important given the traditionally secretive nature of the FISC and its opinions, and ensures the special Article III court applies the standards passed by Congress in an appropriate manner. Furthermore, the Inspectors General of the Department of Justice and intelligence agencies must submit findings to Congress identifying the number of intelligence reports that contain references to U.S. persons twice per year.

Thus, through a series of amendments, revisions and drafts, the U.S. Congress has developed an array of oversight mechanisms designed to monitor the activities of the intelligence community in a manner that does not handicap its ability to effectively address threats to national security. Turning to the United Kingdom, just as FISA was developed in response to litigation and calls for greater oversight of electronic surveillance in the U.S., the RIPA was drafted to address statutory shortcomings in its communications intercept policies under review in a case before the European Court of Human Rights.


The Interception of Communications Act remained the principal legislative guidance for wiretapping and electronic surveillance in the U.K. until _Halford v. United Kingdom_ exposed
shortcomings of the procedures defined within statute that threatened repeated violation of Article 8(1). The U.K. responded to the holding and the possibility that its police conduct would be found in violation of the ECHR without more comprehensive and explicit statutory authorization by drafting new legislation to govern electronic surveillance. Although the objective was arguably to bring U.K. wiretapping practices into compliance with the privacy provisions of Article 8, it must be remembered that doing so did not require limiting government surveillance. To comply with Article 8, the government needed only to give such activity a statutory backing. Thus, resulting legislation was more an expansion of government powers to conduct electronic surveillance than an implementation of safeguards to protect individual privacy.

Similar to the U.S., prior authorization of an operation to intercept electronic communications must be obtained under RIPA, but in the U.K., approval comes from the Executive, rather than the judicial branch. Thus, for communications intercept operations, the Secretary of State must believe that the activity is necessary for national security, crime prevention and detection, or the economic well being of the U.K., and that the authorized activity is proportionate to the fulfillment of those purposes. Additional consideration must be given to whether the information sought through the interception of electronic communications could be reasonably obtained by other, less intrusive means. Furthermore, to prevent general trawling for information, the interception warrant must specify either an individual target of the electronic surveillance, or particular premises, as well as other features that may be used to identify the communications to be intercepted.

To facilitate the execution of interception warrants, the Secretary of State is permitted to require telecommunications operators, such as ISPs, to maintain the capacity to cooperate with
such authorizations. The telecommunications providers’ ability to cooperate is based upon three factors: (1) the ability to meet RIPA’s requirements for protection of intercepted material from disclosure; (2) the ability to maintain confidentiality; and (3) the ability to carry out functions required in the interception of communications. Where it appears that a provider lacks the technical capacity to ensure the interception and transmission of electronic communications is kept confidential and protected against public disclosure, the Secretary of State may require the installation of means capable of meeting those needs. Though the purpose of such provisions was to ensure greater privacy of electronic communications by limiting the likelihood of public disclosure, the general sentiment perceived the government installation of such means as a carte-blanche to intercept all communications.

In addition to requiring that the ISPs be capable of collecting and transmitting intercepted communications, RIPA includes provisions requiring the disclosure of encryption keys for electronically-protected data. Telecommunications operators are obligated to decrypt a message prior to transmission if they are capable of doing so, and law enforcement is authorized to demand an encryption key if access to the information is deemed necessary. Failure to cooperate with law enforcement when capable of doing so is punishable as a criminal offense under RIPA.

Along with the expanded powers of the government to intercept communications provided for in RIPA, the legislation also included a number of oversight provisions. Four commissioners are tasked with overseeing various aspects of the police, security and intelligence services, replacing similarly positions previously appointed under the Security Service Act 1989 and the Intelligence Services Act 1994. The Interception of Communications Commissioner is tasked with reviewing the performance of the Secretary of State regarding the issuance of
interception warrants, while the Intelligence Services Commissioner monitors the activities of
the intelligence services and the Secretary of State’s duties related to those agencies. Each
commissioner is required to provide an annual report to the Prime Minister detailing the contents
of his oversight activities, and the Prime Minister, in turn, presents the report to Parliament, with
exclusions of sensitive materials when necessary.

The Prime Minister’s authority to exclude sensitive information from the reports
submitted to Parliament presents a serious hindrance to the effective oversight of the intelligence
services and the communications intercept operations. First, the grounds under which the Prime
Minister may exclude information in the reports are identical to areas of authority granted to the
security and intelligence services in their statutory mandates. If information related to the
specific areas where the services are statutorily-authorized to act is excluded from reports
presented to Parliament, then a significant portion of material relevant to effective oversight is
never provided to a government body other than the branch authorizing such activity.

To address complaints raised relating to alleged violations of the Human Rights Act and
claims of unlawful conduct by the intelligence services relating to the interception of
communications or other surveillance, RIPA established the Investigatory Powers Tribunal with
exclusive jurisdiction over such issues. With its authority to hear complaints relating to
alleged violations of the Human Rights Act, the Tribunal was the first domestic body capable of
remedying infringements of the rights protected by the ECHR.

However, because it had exclusive jurisdiction over such complaints, the Tribunal had the
effect of stifling information about the complaints from public disclosure. Even a complainant
receives only minimal information relating to his claims, as the Tribunal will simply issue a
statement declaring either that a determination had been made in his favor, or that no such
determination had been made.\textsuperscript{145} For judgments in favor of the complainant where the violation arose from an act of the Secretary of State or conduct pursuant to a warrant, the Tribunal presents a report of its findings to the Prime Minister, but no further disclosure is required.\textsuperscript{146} In this way, the proceedings of the Tribunal are very similar to those of the U.S. FISA Court, although the latter is subject to greater oversight than the former.\textsuperscript{147}

In sum, though both FISA and RIPA offer relatively broad authority to implement electronic surveillance and communications intercept operations, the U.S. statute balances that concession to law enforcement with more robust oversight mechanisms to monitor and control such activities. This is not surprising, given the relatively short history of intelligence oversight in the U.K. compared to the longer shelf life of FISA and other legislative controls. Thus, it seems the U.S. has benefited from experience with various scandals and abuses of power and emerged with an oversight regime capable of balancing the needs of law enforcement with the interests of personal liberties. Likewise, it seems probable that the system of legislative oversight in the U.K. will gradually grow stronger as time passes and the need for parliamentary restraints on the intelligence services becomes more apparent from either public demands or internal concessions from other branches of the government.

V. Modern Developments and Conclusion

Following the recent shootings at the Fort Hood military base in Texas by Army Major Nidal M. Hasan, news reports revealed that U.S. intelligence agencies had intercepted numerous email messages sent by Hasan to a radical Muslim cleric, Anwar al-Aulaqi, residing in Yemen.\textsuperscript{148} Since news of the prior scrutiny of Hasan’s communications with the cleric first broke, several calls have come from Congress for hearings to investigate the actions of the
intelligence agencies. Interestingly, the calls for review have focused on the failure of the intelligence agencies to act on the intercepted information, rather than on the interception itself.

Some notable points must be addressed regarding the interceptions in this case. First, both the sender and recipient of the communications were U.S. citizens. To be valid under FISA (as amended by the FAA), the surveillance of U.S. citizens is lawful only under a warrant from the FISC based on probable cause that the target is an agent of a foreign power, and then only if a substantial purpose of that surveillance is to acquire foreign intelligence information. No mention has been made whether the surveillance was conducted pursuant to a FISA warrant, but it seems clear that a court order was needed to monitor al-Aulaqi’s email account, and even more so to intercept communications sent by Hasan, a U.S. citizen, from within the U.S.

Additionally, despite clear indications that the interceptions included content-based reviews of entire messages sent by Hasan, little mention has been made of the intrusive surveillance measures implemented by the intelligence agencies. Rather than questioning the authority of the agencies to read the content of private messages sent between U.S. citizens, the inquiry seems to be focused on why more wasn’t done. Though a single incident is a far cry from proof-positive of an endemic shift in privacy expectations, it exemplifies the willingness of society to welcome intrusive surveillance measures when the targets are criminals, but the shock when such means are turned against the general public.

In the U.K., plans to develop a call-log database that would record the details of phone calls and email messages sent and received by citizens were put on hold in 2008 following vocal opposition to the system. The proposal was part of an effort to give the police and security services the capacity to keep pace with technological developments that facilitated faster communications, and was defended as essential to combating terrorism, but opponents labeled
the plan “Orwellian.” The delay was only temporary, however, as reports emerging in November 2009 indicated that the plan to monitor all phone calls and Internet usage was underway, though the single database concept had been abandoned.

The new law, known as the Intercept Modernisation Programme, required all telecommunications companies and ISPs to record the personal communications of their customers, including the date, time and recipient of calls logged, as well as the websites visited. The information is accessible by various public bodies, and the interceptions require only the authorization of a senior police officer, rather than a warrant. The new law increases the power of officials acting under RIPA to obtain greater amounts of personal data, but continues to face significant public opposition. Given the easily-circumvented provisions of Article 8 in the ECHR, however, it appears that so long as the authorities act within the statutory guidelines of the new program, it will be difficult to successfully argue a violation of the Human Rights Act.

In sum, the frameworks for legislative oversight of the intelligence function in the U.S. and U.K. are noticeably different, but a valid comparison is difficult given the relatively recent advent of such functions in the latter, and the more robust history of scrutinizing government conduct in the former. Recent developments in both indicate a shift toward greater government power to implement electronic surveillance and communications intercept operations, but the mechanisms of oversight persist, as well.

It is interesting that the shortcomings of parliamentary oversight in the U.K. are, essentially, self-inflicted wounds, since the provisions limiting access to resources and information pertinent to the intelligence oversight function are included within the statutes passed by Parliament. Effective legislative oversight depends upon a “genuine willingness” to
actively approach the function of monitoring intelligence service activities, and Parliament must assert such an attitude if it hopes to fulfill that role. Likewise, a similar willingness to engage the intelligence agencies must be sustained in the U.S. so that the conduct of the government operates within the parameters of the Constitution.

With the implementation of appropriate mechanisms to restrain the actions of the intelligence services without handcuffing their capacity to effectively operate in the face of new challenges, the parliamentary bodies of the U.S. and U.K. can balance the interests of privacy and security. The populace relies upon the representational bodies of the government to defend the liberties and protections afforded in a democratic society, and that must be the goal of legislative oversight of the intelligence function.

1 For an excellent review tracking the online terror network that planned, coordinated and executed the devastating attacks in the United States on September 11, 2001, see Vladis E. Krebs, *Uncloaking Terrorist Networks*, FIRST MONDAY, Vol. 7, No. 4 (Apr. 2002) available at http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/941/863. The article mapped the relational electronic network between the 9/11 hijackers to demonstrate how data mining technologies, discussed infra, are useful to uncover threats to national security using public data from Internet communications.

2 See Paul Rosenzweig, “Proposal for Implementing the Terrorism Information Awareness System,” Center for Legal and Judicial Studies, The Heritage Foundation (2003) available at http://www.heritage.org/Research/homelanddefense/1m8.cfm (noting that data mining technologies can be designed to render effective results without threatening American civil liberties by incorporating built-in safeguards to limit the possibility of abuse).


4 See Fourth Amendment Issues Raised by the FBI’s “Carnivore” Program: Hearing Before the Subcomm. on the Constitution of the H. Comm. on the Judiciary, 106th Cong., 2d Sess. (July 24, 2000) [hereinafter House Carnivore Hearing]; The “Carnivore” Controversy: Electronic Surveillance and Privacy in the Digital Age: Hearing Before the S. Comm. on the Judiciary, 106th Cong., 2d Sess. (Sept. 6, 2000) [hereinafter Senate Carnivore Hearing]. The inquiries by the congressional committees are perhaps better viewed as exercises of legislative oversight in form rather than substance, because though the FBI ultimately had to justify its implementation of the Carnivore program before Congress, no substantive developments emerged from the proceedings.


6 Id. at 7.

7 Id.

8 Id.

9 Id.
In the House hearing, FBI testimony focused primarily on emphasizing the truly narrow scope of its investigations using Carnivore, highlighting the filter mechanisms and other safeguards in place, along with the already extensive oversight of its operations from within the FBI, through the DOJ, and by Congress. See House Carnivore Hearing, supra note 4, at 7-14 (statement of Donald M. Kerr, Director, Lab Division, FBI); see id. at 14-15 (statement of Larry R. Parkinson, General Counsel, FBI). The ACLU countered by calling into question the statutory authorization for the FBI’s widespread electronic surveillance and warning against accepting its “trust us” argument that it thoroughly oversees and audits its use of Carnivore, particularly given past incidents of abuse. See id. at 45-56 (statement of Barry Steinhardt, Associate Director, ACLU).

In the Senate, the FBI again outlined the safeguards and filter mechanisms it employed to limit the scope of its surveillance, but also addressed the threats and challenges presented by increased use of electronic communications by criminals and terrorists. See Senate Carnivore Hearing, supra note 4, at 9-21 (statement of Donald M. Kerr, Director, Lab Division, FBI). On the other hand, privacy interests were addressed through...
invocations of Supreme Court Justice Douglas’ “fundamental right to be left alone,” and noted that regardless of the technological advancements, the core principles of the Constitution remained the foundation on which the U.S. stood, including the preservation of privacy. See id. at 36-42 (statement of Michael O’Neill, Asst. Prof. of Law, George Mason University Law School).

22 See Fed. Bureau of Investigation and U.S. Dept. of Justice, Carnivore/DCS-1000 Report to Congress: Submitted to Judiciary Committees of the U.S. House of Representatives and U.S. Senate, Apr. 24, 2003 (reporting that the FBI used commercially-available software to conduct electronic surveillance five times in 2002, and did not use Carnivore at all); see Fed. Bureau of Investigation and U.S. Dept. of Justice, Carnivore/DCS-1000 Report to Congress: Submitted to Judiciary Committees of the U.S. House of Representatives and U.S. Senate, Dec. 18, 2003 (reporting that the FBI used commercially-available software to conduct electronic surveillance on only eight occasions in 2003, and did not use Carnivore at all); see also Caron Carlson, “FBI’s Carnivore is Toothless,” EWEEK, Vol. 22, Iss. 4, Jan. 24, 2005 at 18 (reporting that the FBI no longer used its Carnivore program to conduct electronic surveillance, opting instead to use commercially-available software).

23 See IITRI Independent Review, supra note 4, at 4.2.1.

24 “The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” U.S. Const. Amend. IV. The case law interpreting and shaping this text is voluminous and beyond the scope of this article, and so we will reach only back to the development of the “reasonable expectation of privacy,” since it was first enunciated in Katz v. United States, 389 U.S. 347 (1967).

25 See generally Her Majesty’s Stationery Office, Report of the Committee on Privacy and Related Matters (“The Calcutt Committee Report”), 1990, Cm. 1102 (U.K.) (finding that a right to privacy lacked statutory definition in English law, and proposing a definition encompassing the right to be protected against intrusion into the personal life or affairs of an individual); see also Her Majesty’s Stationery Office, Government Response to the National Heritage Select Committee: Privacy and Media Intrusion, 1995, Cm. 2918 (U.K.) (recognizing the right of the person to be free from harassment, and a right to privacy of personal information and communications).

The Human Rights Act 1998 incorporated the provisions of the European Convention on Human Rights into domestic law, which included a right to privacy in Article 8. THE HUMAN RIGHTS ACT, 1998, c. 42, Sched. 1, Art. 8. Entitled “Right to Respect for Private and Family Life,” it states “Everyone has the right to respect for his private and family life, his home and his correspondence.” Id. at Art. 8(1). By incorporating the ECHR, the U.K. not only bound itself to uphold its provisions, but also to abide by the judgments of the European Court of Human Rights and to ensure its national legislation is compatible with those holdings. Id. at Art. 3.

26 Compare U.S. CONST., Amend. IV, with THE HUMAN RIGHTS ACT, supra note 27, at Art. 8. The Fourth Amendment is classified as a “negative” right, i.e., a protection against unreasonable government intrusion, rather than a “positive” right, such as Article 8’s assurance of respect for the private life of the individual, absent a government interest in national security, national economic well-being, crime prevention, or public health and welfare.

27 See Olmstead v. United States, 277 U.S. 438 (1928). Prior to Katz, the primary consideration in cases alleging violations of the Fourth Amendment was whether a physical trespass had occurred.

28 Katz, supra note 26, at 351. This development was particularly important because the individual’s Fourth Amendment rights no longer depended upon his presence in a constitutionally-protected space, such as the home, but rather followed wherever the person went. Katz involved the use of an electronic listening device, in the absence of a warrant, to monitor the defendant’s conversations placed from a public telephone booth, and evidence obtained from that surveillance was ultimately used to convict him of a federal offense for transmitting wagering information from Los Angeles to Miami and Boston. Id. at 348.

31 Id. at 357 (“… [S]earches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment….”). For more cases exploring the importance of a “neutral and detached” judicial officer to issue the warrant, see, e.g., Coolidge v. New Hampshire, 403 U.S. 443, 450 (1971); United States v. Chadwick, 433 U.S. 1, 9 (1977); Lo-Ji Sales, Inc. v. New York, 442 U.S. 319, 327 (1979). Unlike the U.S. reliance on court orders issued by judicial officers, surveillance warrants in the U.K. are issued by the executive authority. Laura K. Donohue, Anglo-American Privacy and Surveillance, 96 J. CRIM. L. & CRIMINOLOGY 1059, 1156 (2006).

32 Katz, supra note 26, at 359 n. 23. As will be discussed further in Part IV, infra, FISA permits the implementation of surveillance measures without a warrant in specific circumstances.
Justice White addressed the national security issue in his concurring opinion to *Katz*. *Id.* at 362 (White, J. concurring). Specifically, he believed that the warrant procedure should not be required where the President or the Attorney General authorized electronic surveillance after considering the requirements of national security. *Id.* at 363-64. Justice White’s opinion was apparently shared by Congress, because FISA, as amended, permits the Attorney General to authorize electronic surveillance without a warrant for up to seven days after weighing the needs of the government, but within that period he must submit an application to the FISA Court certifying that appropriate safeguards are in place and seek judicial approval of the operation. 50 U.S.C. §1805(e), as amended. 33 *See Katz,* supra note 26, at 360 (Harlan, J. concurring).

Id. at 361 (Harlan, J. concurring).

For criticism of the subjective expectation of privacy prong of Justice Harlan’s Fourth Amendment test, see Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349 (1974).

36 *See 50 U.S.C. §1881c(2).* The FISA Amendments Act of 2008 explicitly prohibits the intentional targeting of a U.S. person located outside the United States for electronic surveillance when that individual has a “reasonable expectation of privacy” that would otherwise require a warrant to be conducted domestically. 37 *Katz,* supra note 26, at 351 (“What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.”).

38 *See Smith v. Maryland,* 442 U.S. 735 (1979). In *Smith,* following the robbery of a victim’s home, she began to receive threatening phone calls from a person identifying himself as the robber, and after police identified a suspect matching the victim’s description of the robber and located his residence, they installed a pen register at the central telephone company office, without a warrant, to monitor the numbers he called. That information ultimately led to a search warrant, and the arrest and conviction of the man for the robbery. *Id.* at 737.

39 *See United States v. Knotts,* 460 U.S. 276, 282-83 (1983) (approving of the warrantless use of a radio-transmitting beeper to track the movements of a can of chloroform in a suspect’s possession as he travelled along public roads, because “nothing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them.”); but see *United States v. Karo,* 468 U.S. 705 (1984) (finding that use of a radio transmitting beeper to track suspect’s movements was permissible until the beeper entered the confines of the home, at which time such use became a warrantless search because movements could not have been observed without entering the home).

40 The Court’s rationale in *Smith* that a legitimate privacy expectation did not exist was dependent upon the conveyance of phone numbers dialed to the telephone company’s switchboard, which is an automated system in modern times, but was historically operated by a human technician. Thus, because the operator would know the numbers connected in any given phone call, they were not hidden from public view. Additionally, it was regular practice for telephone companies to keep records of phone numbers dialed, which were sent via monthly billings to subscribers, so the phone user would surely have been aware that the numbers he dialed were recorded in some manner, and he therefore lacked a legitimate expectation of privacy. *Smith,* supra note 38, at 742.

Similarly, in *United States v. Knotts,* police surveillance using the radio-transmitting beeper was only used to track the suspect’s movements along public roads, and such activity lacked a legitimate expectation of privacy to render the surveillance an impermissible search violating the Fourth Amendment. *Knotts,* supra note 39, at 283. Subsequently, *United States v. Karo* distinguished *Knotts* because the warrantless use of the radio-transmitting beeper in that case tracked the suspect’s movements both in publicly-viewable spaces and later within his home, leading the police to acquire information that could not otherwise have been obtained without entering the dwelling. *Karo,* supra note 39, at 705.


42 *Kyllo,* supra note 41. During the course of an investigation of suspected marijuana growth within a suspect’s home, police officers, acting without a warrant, used a thermal-imaging device to measure heat signatures emanating from the home, which identified halide lamps and led to the arrest and conviction of the individual. *Id.* at 29-30.

43 *Id.* at 34, 40. The key distinction was that the technology permitted police to observe the interior of the home that would not otherwise be viewable without a physical entry. Such intrusive technology could be said to effect a constructive trespass of the home, the most guarded of places in Fourth Amendment jurisprudence.

Justice Stevens dissented from the Court’s holding on this point because the proposed rule was not as solid as the majority claimed. The caveat regarding the public availability of the technology employed served only to undermine the effectiveness of the Court’s rule, because the use of such intrusive technology would arguably be allowed if it were in wide public use. *See id.* at 47 (Stevens, J. dissenting).
44 Ostensibly, the greater availability or use a particular piece of technology has, the more aware the general public will be of its capacity, and the more likely it is that the individual expectation of privacy will be diminished accordingly. But should the individual’s awareness of an intrusive technology have any bearing on the objective reasonableness of a private activity that it affects? Though the thermal-imaging technology employed in Kyllo was not widely-available for public use, commercial data mining and electronic surveillance software were publicly-available at the time of Carnivore’s implementation. It would seem from the reaction to the disclosure of the FBI’s use of the Carnivore program that the subjective expectation of privacy is not minimized simply because such technologies are available to, and in use by, the general public. Kyllo may have ultimately been one step forward and two steps backward for Fourth Amendment privacy interests by securing for law enforcement a justification for the warrantless use of surveillance technologies.

Following the intense scrutiny surrounding its use of the Carnivore program, the FBI supposedly abandoned its implementation began to use the commercially-available alternatives to conduct its electronic surveillance. Carlson, supra note 24, at 18. Interestingly, as noted in the IITRI Independent Technical Review, Carnivore presented a more attractive option than commercially-available software because of its built-in safeguards and the protocols in place regarding its implementation. IITRI Independent Review, supra note 4, at 4.2.1.

A simple search of Google will reveal thousands of commercially-available software options to monitor personal and business computer usage, many of which are now available to download free-of-charge.

45 See Katz, supra note 26, at 357 (“… [S]earches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment…”).
46 See, e.g., Id. at 351; Smith, supra note 38, at 742; Knotts, supra note 39, at 282-83; Karo, supra note 39, at 705.
47 The standard remedy for violations of the Fourth Amendment is known as the “exclusionary rule,” which effectively excludes evidence obtained as a result of the unconstitutional search from admission at trial. See Mapp v. Ohio, 367 U.S. 643 (1961).
48 HUMAN RIGHTS ACT, supra note 27, at Art. 8(2).
49 Dept. for Constitutional Affairs, A Guide to the Human Rights Act 1998: Third Edition, Oct. 2006, at 5 [hereinafter Guide to the Human Rights Act]; see HUMAN RIGHTS ACT, supra note 27. Prior to the incorporation of the ECHR into domestic law, parties in the U.K. were free to raise claims alleging a violation of its provisions, but could only have their claims heard before the European Court of Human Rights. With the passage of the Human Rights Act 1998, domestic courts were obligated to uphold the provisions of the ECHR, where previously the articles were merely persuasive authority to be considered in the absence of national legislation. Guide to the Human Rights Act at 5.
50 Id. at 13.
51 Id. at 6. Higher courts are permitted to make a “declaration of incompatibility” if primary legislation contravenes a Convention right, but such a ruling is essentially a persuasive judgment intended to encourage Parliament to make appropriate changes to the law, because it has no bearing on the continuing validity or enforceability of the legislation. See HUMAN RIGHTS ACT, supra note 27, at Sec. 4(2)-(6).
52 Id. at Sec. 6(2); Id. at Sched. 1, Art. 8(2) (“There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.”).
53 Interestingly, the Security Service Act 1989 and the Intelligence Services Act 1994 were enacted to give the security and intelligence services in the U.K. a statutory basis specifically to avoid violating the terms of the ECHR. By establishing a statutory mandate for each agency, their operations were conducted “in accordance with the law,” and thus qualified for the exception provision in Article 8(2). Donohue, supra note 31, at 1158.
that the interception of calls made from an office telephone violated Article 8 because it was performed outside the scope of the relevant law and because the caller would have had a reasonable expectation of privacy in making the calls).

See Perry, supra note 55. Perry involved the covert videotaping of a criminal suspect after he had refused to take part in a lineup, which was held by the European Court of Human Rights to violate his Article 8 right to respect for private life. The basis for the Court’s ruling was that the videotaping was not within the normal use of cameras in the police station, and the action was not authorized by the law or established protocol.

Since the widespread implementation of the Closed-Circuit Television (CCTV) network, videotaping surveillance has become a fairly commonplace occurrence in the U.K. Though not specifically authorized by The Data Protection Act 1998, the terms of the statute clearly provide for the kinds of information captured by CCTV. The recording of video images had serious implications for the Human Rights Act 1998 because covert surveillance would contravene the privacy interests protected by the statute. As a result, CCTV systems must now be accompanied by “adequate signage” to alert civilians to their presence. Nick Taylor, Regulating Big Brother: The U.K. Approach (University of Leeds – School of Law (2007) available at http://ssrn.com/abstract=999686. The signage requirement may be avoided if the CCTV system is employed primarily for crime detection and prevention, however – two interests specifically identified in Article 8 as sufficient to circumvent the obligation to respect private life. DATA PROTECT ACT, 1998, c. 29, Sec. 29.

See Katz, supra note 26, at 361 (Harlan, J. concurring).

DCAF Backgrounder, supra note 20.

See Hans Born and Ian Leigh, MAKING INTELLIGENCE ACCOUNTABLE: LEGAL STANDARDS AND BEST PRACTICES FOR OVERSIGHT OF INTELLIGENCE AGENCIES at 17 (Publishing House of the Parliament of Norway 2005) (“Only if security and intelligence agencies are established by law and derive their powers from the legal regime can they be said to enjoy legitimacy. Without such a framework there is no basis for distinguishing between actions taken on behalf of the state and those of law-breakers, including terrorists. ‘National security’ should not be a pretext to abandon the commitment to the rule of law which characterises democratic states, even in extreme situations.”).

Donohue, supra note 31, at 1077 (referring to hearings held by the Senate Subcommittee on Administrative Practices and Procedures in 1964, led by Senator Edward V. Long, which looked into the executive practice of conducting domestic surveillance).


Id. at 214. Title III differentiated foreign surveillance from domestic investigations by explicitly reserving for the President all powers necessary to obtain foreign intelligence information essential to national security. Id. This is noteworthy because it was the availability of this authority to act in the interest of national security that proved to be the largest loophole in Title III’s warrant requirements, and ultimately led to the enactment of FISA a decade later.
information obtained from electronic surveillance under authorization of the Attorney General, but without prior court approval. Id. at 299-300.

71 Id. at 320 (“We recognize, as we have before, the constitutional basis of the President’s domestic security role, but we think it must be exercised in a manner compatible with the Fourth Amendment. In this case we hold that this requires an appropriate prior warrant procedure.”).


73 Id. at Book I, 5 (“Too many people have been spied upon by too many Government agencies and to [sic] much information has been collected.”).

74 Id. at 137 (“The legal questions involved in intelligence programs were often not considered. On other occasions, they were intentionally disregarded in the belief that because the programs served the “national security” the law did not apply.”).


The government’s authority to intercept communications was considered in 1957 by a committee appointed to look into rampant wiretappings conducted by the police, but concluded that such power was “obscure.” Birkett Committee Report at ¶9. Despite such unclear foundations, the committee nonetheless argued that wiretappings should be permitted to continue given their effectiveness in detecting major crime and preventing threats to national security. Id. at ¶¶107-113. However, the committee emphasized that specific conditions should be met prior to authorization to obtain a wiretapping warrant, which included that the offense be serious; normal methods of investigation had failed, or were unlikely to succeed; and there was good reason to think the interception would result in a conviction. Id. at ¶64. This last recommended condition is similar to the establishment of the “probable cause” standard as the necessary legal component to obtain a court order under Title III, which would have been an important requirement to impose upon law enforcement, but the committee report and its recommendations were not encapsulated in any subsequent legislation by Parliament.

76 Malone, supra note 55, at 14 (referencing Article 8(2) of the ECHR, which requires that actions taken in contravention to the provisions for respect of the individual’s private life must be conducted “in accordance with the law” in order to be permissible infringements of that right). Although the U.K. had not yet incorporated the provisions of the ECHR into its domestic law, which it would later do through the Human Rights Act 1998, it was nonetheless obligated to follow its terms and the holdings of the European Court of Human Rights to the best extent possible. While not technically a binding decision, it was still in the best interest of the U.K. to follow the Court’s decision and enact legislation to give a statutory basis for its wiretapping activities in order to avoid subsequent litigation before the Court on the same issue.

Recognizing the necessity of a statutory basis to comply with the terms of the ECHR, Parliament subsequently enacted the Security Service Act 1989 and the Intelligence Services Act 1994. SECURITY SERVICE ACT, 1989, c. 5; INTELLIGENCE SERVICES ACT, 1994, c. 13. Prior to the enactment of such legislation, the Services acted under authority of the Royal Prerogative, a residual common law power of the Crown, but technically lacked a legal basis for such operations that would be recognized by the European Court of Human Rights. Ian Leigh, Accountability of Service and Intelligence in the United Kingdom, in WHO’S WATCHING THE SPIES? ESTABLISHING INTELLIGENCE SERVICE ACCOUNTABILITY at 79, 80 (Hans Born, Loch K. Johnson, and Ian Leigh eds., 2005).

77 INTERCEPTION OF COMMUNICATIONS ACT, 1985, c. 56. With the passage of the two acts, the Services were given a statutory mandate under which they could conduct surveillance without violating the provisions of the ECHR. Id.

78 Yeates, supra note 75, at 133.

79 Id.


81 Donohue, supra note 31, at 1094.

82 “Foreign intelligence information” is defined within the statute as information that relates to the capacity of the U.S. to protect against an actual or perceived attack, or clandestine intelligence activities carried out by a foreign power or its agents within the U.S. The definition also extended to information pertaining to a U.S. person that was necessary to the national security or the foreign affairs of the U.S. 50 U.S.C. §1801(e)(1)-(2).

83 Agents of foreign powers are defined as non-U.S. persons acting as an employee, or on behalf, of a foreign power, as well as persons (including U.S. persons) knowingly engaged in clandestine intelligence gathering activities on
behalf of or pursuant to the direction of a foreign intelligence service or power. 92 Stat. 1783, 1784, codified at 50 U.S.C. §1801(b)(1)-(2). However, Congress explicitly noted that a U.S. person could not be considered an agent of a foreign power “solely upon the basis of activities protected by the first amendment to the Constitution....” 92 Stat. 1783, 1790, codified at 50 U.S.C. §1805(a)(3)(A).


85 92 Stat. 1783, 1786, codified at 50 U.S.C. §1802(a)(1). Given that the surveillance was conducted without a warrant, it was important that a U.S. person was not a likely target because of the Fourth Amendment’s warrant requirements when an individual held a reasonable expectation of privacy. See 92 Stat. 1783, 1785, codified at 50 U.S.C. §1801(f). A U.S. person could be targeted under FISA, but only upon a determination of probable cause that he or she was engaged in illegal activities on behalf, or under the instruction, of a foreign power or agent, which would justify the issuance of a court order for such surveillance. 50 U.S.C. §1801(b)(2).

86 92 Stat. 1783, 1791, codified at 50 U.S.C. §1805(e). The emergency circumstance must have been of such a nature that the immediacy of the need to implement surveillance measures left no time to obtain prior judicial approval. The Attorney General must also have determined that the facts of the case were sufficient that a valid court order would have otherwise been granted had the exigency not required immediate action. Id.

87 Id. Without judicial approval of surveillance after submission of the request to the FISC, the operation had to be terminated within 24 hours, or as soon as the information sought was obtained, whichever was earliest. Additionally, if the subsequent application were denied, any information obtained during the initial emergency authorization period had to be excluded from evidence pursuant to the judicially-created exclusionary rule. Id.

The permissible period of warrantless surveillance under the exercise of emergency powers was subsequently extended to 72 hours in the PATRIOT Act, and extended further to seven days under the FISA Amendments Act of 2008.

88 92 Stat. 1783, 1788-89, codified at 50 U.S.C. §1804(a)(1)-(11). “The purpose” of obtaining foreign intelligence information was understood to mean that the surveillance was conducted for the primary purpose of acquiring such information, though subsequent amendments to FISA altered this language.

89 Id. Similar to Title III, FISA implemented the probable cause standard as the necessary legal determination to issue a warrant for electronic surveillance to acquire foreign intelligence information.

90 Id.


92 Unlike the legislative history surrounding the passage of FISA, see Joint Explanatory Statement of the Committee of Conference, H. Conf. Rep. No. 95-1720 (1978), the PATRIOT Act was enacted without committee hearings, conference reports or other traditional references of the legislative process. For an excellent resource of the legislative history leading up to the passage of FISA, visit the Center for National Security Studies website devoted to the statute available at http://www.cnss.org/fisa.htm.

The PATRIOT Act was passed under demands from Attorney General John Ashcroft to broaden government authority to conduct electronic surveillance of terrorism suspects, and the ominous threat of another terrorist attack. Incrédibly, the legislation passed both Chambers of Congress by overwhelming votes and without substantive debate in a mere 18-hour period. Robin Toner and Neil A. Lewis, “House Passes Terrorism Bill Much Like Senate’s, but with 5-Year Limit,” N.Y. TIMES, Oct. 13, 2001, at B6. The Act was largely in reaction to revelations of the vital role the Internet had played in organizing and coordinating the attacks, as well as the failure of U.S. intelligence, security and law enforcement agencies to analyze and share information of the hijackers’ activities that was spread across their respective databases. See David S. Falls and Ariana Eunjung Cha, “Agents Following Suspects’ Lengthy Electronic Trail: Web of Connections Used to Plan Attack,” WASH. POST, Oct. 4, 2001, at A24; Stacy Blasberg, Law and Technology of Security Measures in the Wake of Terrorism, 8 B.U. J. Sci. & Tech. L. 721, 721 (2002) (referencing statements made by George W. Bush in his budgetary report, “Using 21st Century Technology to Defend the Homeland”).


95 Id. The alteration is substantial, because it ostensibly permits the government to use FISA instead of Title III to authorize a wiretap, even if the primary subject matter of the surveillance would have otherwise fallen under the jurisdiction of the latter.
In re Sealed Case No. 02-001, 310 F.3d 717, 732-35 (2002) (“The addition of the word “significant” to section 1804(a)(7)(B) imposed a requirement that the government have a measurable foreign intelligence purpose, other than just criminal prosecution of even foreign intelligence crimes…. So long as the government entertains a realistic option of dealing with the agent other than through criminal prosecution, it satisfies the significant purpose test.”). The effect of this interpretation was to recognize that the government need not make the acquisition of foreign intelligence information its primary target in an operation, but rather only a secondary objective, in order to be statutorily authorized.


See id. (referring to several “senior government officials” interviewed on the condition of anonymity who expressed concerns that the NSA program was an illegal operation).

The program was particularly significant because the NSA’s traditional jurisdiction focused solely on foreign communications, an area outside the scope of FISA governance, but under the Executive Order it was expanded to include domestic communications sent internationally. The interception of such domestic communications typically required a court order pursuant to FISA, but under the NSA program, no such limitations were in place.


Id. at §105B(a), codified at 50 U.S.C. §1805b.

The PAA was short-lived due to widespread criticism of both the manner in which it was enacted and the broad authority it granted within its provisions. See, e.g., Carl Hulse, “House Leaves Surveillance Law to Expire,” N.Y. TIMES, Feb. 15, 2008, at A17 (reporting that the option to extend the provisions of the PAA was foregone at the end of its six-month term); James Risen and Eric Lichtblau, “Concerns Raised on Wider Spying Under New Law,” N.Y. TIMES, Aug. 19, 2007, at A1 (noting the “frenetic, end-of-session scramble” to enact the legislation without concerted efforts by Congress to fully understand the statute prior to its passage); Charlie Savage, “New Law Expands Power to Wiretap – Diminishes Oversight of NSA Spy Program,” BOSTON GLOBE, Aug. 6, 2007, at 1A (noting that the majority of the PAA was drafted by the White House, and the bill received no committee hearings prior to its passage). The PAA, like the PATRIOT Act, is an example of legislation approved by Congress at the behest of the Executive Branch without demanding sufficient time for the provisions of proposed legislation to be vetted in committee hearings or floor debates.

Effective legislative oversight depends upon a genuine interest of legislators to actively engage and evaluate proposals for expanding the authority of intelligence and security services by congressional committees and the legislature as a whole is a fundamental and necessary component of effective oversight. DCAF Backgrounder, supra note 20. Unfortunately, once again, Members of Congress were more willing to acquiesce to Executive pressure than to be portrayed as “weak on terrorism.” Ellen Nakashima, “A Push to Rewrite Wiretap Law,” WASH. POST, Aug. 1, 2007, at A4 (reporting Bush Administration use of the approaching August congressional recess and portrayals of opposition to the bill as being “weak on terrorism” to pressure approval); see also James Risen, “Democrats Scrambling to Expand Eavesdropping,” N.Y. TIMES, Aug. 1, 2007, at A12.


The provisions recognized by the FAA pertain to the protection of privacy in wire, oral and electronic communications, and regulate the circumstances under which such transmissions may be intercepted within the U.S. for criminal investigation purposes, codified at 18 U.S.C. §2510 et seq.

The first statute referred to protects the privacy of stored wire and electronic communications, as well as law enforcement access to such resources, codified at 18 U.S.C. §§2701 et seq. The other statute regulates the use of pen registers, trap and trace operations, and similar interceptions of transactional information other than the contents of a communication, codified at 18 U.S.C. §§3121 et seq.


Fishman and McKenna, supra note 84, at 12-16.


As originally enacted, FISA only governed electronic surveillance targeting persons and places within the U.S. However, the disclosure of the President’s NSA spy program revealed a shortcoming in the statutory framework regulating electronic surveillance – the lack of legislative provisions governing the interception of communications occurring outside the U.S. Given that such operations were already taking place, the only logical choice would be to authorize the electronic surveillance of international communications, but control the circumstances in which such operations could be lawful. From the perspective of legislative oversight of intelligence operations, this seems the most plausible reason behind the expansions included within the FAA.
11 Id. at §1881a(b), (i). The certification that surveillance does not indirectly target a person known to be in the U.S. was designed to prevent the government from targeting a person living abroad with the purpose of monitoring the communications of a person residing within the U.S. Thus, to implement lawful surveillance under this section, the government must make every effort to ensure that it does not intentionally target U.S. persons and others residing within the U.S.
12 Id. at §1881a(d)(1)(A).
13 Id. at §1881a(a).
14 See Id. at §§1881b, 1881c.
15 Id. at §1881(b)(1)(C)(i)-(ii); see also SSCI Report, supra note 108, at 15.
16 This provision is particularly interesting given the nature of electronic information streams through networks, because modern communications transmitted through the Internet are sent through a routing station on their way to an intended recipient, but protocols built into the system direct data through the hub with the greatest present capacity. U.S. Congress, Office of Tech. Assessment, Electronic Surveillance in a Digital Age, OTA-BP-ITC-149 at 2, 4 (U.S. Gov’t Printing Office, July 1995). In effect, an email sent between neighbors in Washington, D.C., may be routed through a server in the United Kingdom on its way to the recipient. If this is the case, the FAA permits the transmission of a targeted U.S. person living abroad to be monitored pursuant to a court order if it travels through a domestic routing server. This becomes relevant if a particular routing server could be constructed to handle massive amounts of electronic data, thus making it a more accessible hub for communications worldwide, and enabling the government to monitor and intercept a much larger stream of data. See Matt Bedan, Echelon’s Effect: The Obsolescence of the U.S. Foreign Intelligence Legal Regime, 59 FED. COMM. L.J. 425, 437-38 (2007) (commenting upon the “Echelon” system of global communications interception and its general capabilities, including the construction of a large routing station in Menwith Hill, England, which is rumored to be capable of intercepting billions of communications each day due to its mammoth fiber optic cable capacity).

Another important provision of the FAA, though not within the scope of this article, was the grant of retroactive immunity from civil litigation for electronic communications providers, i.e. ISPs and phone companies, that had cooperated with the NSA in its surveillance activities conducted under the executive order issued in 2002. See 50 U.S.C. §1881a(h)(3). This provision was a divisive issue, given the highly controversial nature of the NSA program, but was nonetheless included within the FAA to dismiss the numerous lawsuits underway against various companies that had cooperated with the program. Eric Lichtblau, “Senate Approves Bill to Broaden Wiretap Powers,” N.Y. TIMES, July 10, 2008, at A1.
18 SSCI Report, supra note 108, at 5. The FISC may issue an order authorizing intelligence service actions upon the establishment of probable cause that the U.S. person to be targeted is an agent of a foreign power. 50 U.S.C. §1881c(b)(3)(B). Under exigent circumstances, the Attorney General may authorize the surveillance of a U.S. person living abroad for up to 7 days without a court order, similar to the “emergency powers” provisions of FISA. Id. at §1881c(d)(1).
19 Katz, supra note 26, at 351.
22 The Attorney General retains the authority to redact material within FISC opinions deemed sensitive or vital to the security of the U.S. 50 U.S.C. §1871(d).
24 REGULATION OF INVESTIGATORY POWERS ACT, 2000, c. 23.
25 See Halford, supra note 55.
26 See Donohue, supra note 31, at 1166-67 (referring to a consultation paper issued by the Home Office in 1999 relating to communications interception that formed the groundwork for subsequent provisions of the RIPA).
27 HUMAN RIGHTS ACT, supra note 27, at Sec. 6(2); Id. at Sched. 1, Art. 8(2) (“There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and
freedoms of others.”). Thus, to comply with the ECHR, the government need only enact legislation validating its own conduct as legal, which would technically make such activity “in accordance with the law.”


128 Regulation of Investigatory Powers Act, supra note 123, at §7(1)(a) (designating the Secretary of State as the issuing authority for interception warrants). Other “senior officials” are permitted to issue such authorizations under emergency circumstances where the Secretary of State has expressly approved of the issuance of a warrant, or for cases relating to the fulfillment of obligations under an “international mutual assistance agreement” where interceptions will take place outside the United Kingdom. Id. at §7(2)(a)-(b).

129 Id. at §5(2)-(3).

130 Id. at §5(4).

131 Id. at §8(1)-(2).

132 Id. at §12(1)-(2).


134 Regulation of Investigatory Powers Act, supra note 123, at §§12(2), (11). These measures are intended to ensure telecommunication operators are capable and ready to handle requests from the police, intelligence and security services when a valid interception warrant is issued.

135 See John Naughton, “Your Privacy Ends Here,” The Observer (U.K.), Jun. 4, 2000 available at http://www.guardian.co.uk/technology/2000/jun/04/internet.observerfocus (noting that under RIPA, MI5 would have access to all online communications, including emails and use history, which would be transmitted instantly to the Government Technical Assistance Centre at its London headquarters through the “black boxes” installed at ISPs); Anonymous, Britain: Being Watched, The Economist, Vol. 356, Iss. 8185, Aug. 26, 2000 at 46 (reporting on the opposition to RIPA by various groups within the U.K., particularly relating to the forced disclosure of encryption keys and the installment of “black box” interception devices at ISPs). For a comprehensive compilation of public criticism against RIPA, including news broadcasts, interviews, and newspaper stories, see Foundation for Information Policy Research (FIPR), “Regulation of Investigatory Powers Information Centre” available at http://www.fipr.org/rip (last accessed 11/30/2009).


137 Id. at §50(1)(b); Id. at §50(2)(a).

138 Id. at §§53-54. Convictions for failure or refusal to cooperate with the disclosure of encryption keys to law enforcement carry a penalty up to two years in prison, though no indication was found that such Draconian measures have been exercised.

139 See Security Service Act, supra note 76, at §§4(1), (3), (4); Intelligence Services Act, supra note 76, at §§8(1)-(7). RIPA created positions for a Chief Surveillance Commissioner, an Interception of Communications Commissioner, an Intelligence Services Commissioner, and a Commissioner for Northern Ireland.

140 Regulation of Investigatory Powers Act, supra note 123, at §§57, 59. Each of the commissioners is assured the full cooperation of officials and members within their respective fields to facilitate the observations, which includes providing all documents and information necessary to fulfill their functions. See id. at §§58, 60.

141 Id. at §§58(4), (6), (7); id. at §§60(2), (4), (5). The Prime Minister is permitted to exclude information from the reports presented to Parliament that he determines would be “contrary to public interest or prejudicial to national security, the prevention or detection of crime, the economic well-being of the United Kingdom, or the continued discharge of functions of any public authority whose activities include activities that are subject to review by that Commissioner.” Id. at §§58(7) and 60(5). See generally Hon. Sir Paul Kennedy, Report of the Interception of Communications Commissioner for 2008, July 21, 2009; Hon. Sir Peter Gibson, Report of the Intelligence Services Commissioner for 2008, July 21, 2009.

142 Compare Regulation of Investigatory Powers Act, supra note 123, at §§58(7) and 60(5) with Security Service Act, supra note 76, at §1(2)-(3) and Intelligence Services Act, supra note 76, at §1(2)(a)-(c).
REGULATION OF INVESTIGATORY POWERS ACT, supra note 123, at §65(2). RIPA established the Investigatory Powers Tribunal to replace the tribunals previously established by the Interception of Communications Act, the Security Service Act and the Intelligence Services Act.

Donohue, supra note 31, at 1172-74. Though domestic courts were often presented with claims of human rights violations or charges against the intelligence services, they were unable to resolve the complaints because there was no statutory guidance governing privacy interests or establishing guidelines for electronic surveillance. With the introduction of the Human Rights Act and RIPA, however, such guidelines were available. However, because the Tribunal was statutorily granted exclusive jurisdiction to hear all such claims, the issues could not be heard in domestic courts yet again, and so details of the complaints were often concealed.

REGULATION OF INVESTIGATORY POWERS ACT, supra note 123, at §68(4)(a)-(b).

Id. at §68(5)(a)-(b).

See FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436, 2460 (requiring the Attorney General to disclose to Congress all FISC decisions that substantially interpret or modify the intended purpose of the FAA).

Philip Rucker, Carrie Johnson and Ellen Nakashima, “Hasan E-Mails to Cleric Didn’t Result In Inquiry,” WASH. POST, Nov. 10, 2009 at A1. The messages were intercepted because intelligence agencies had been monitoring the email of al-Aulaqi. From December 2008 through early-2009, between 10 and 20 messages were scrutinized by a joint terrorism task force led by the FBI, but the content of the communications reportedly did not merit further investigation. See id. (reporting that the content of messages sent by Hasan primarily pertained to the topic of his academic research, but also included “social chatter and religious discourse”); BBC News Staff Writer, “U.S. Major Contacted Radical Cleric,” BBC News, Nov. 10, 2009 available at http://news.bbc.co.uk/go/pr/fr/-/hi/americas/8351740.stm (reporting that the email account of al-Aulaqi had been under surveillance by intelligence agencies, but that the content of Hasan’s messages did not threaten violence).

See BBC News Staff Writer, “U.S. Senate May Probe Army Shooting,” Nov. 8, 2009 available at http://news.bbc.co.uk/go/pr/fr/-/hi/americas/8349413.stm (reporting that Senator Joe Lieberman, Chair of the Senate Homeland Security Committee, has called for an investigation into the events surrounding the shooting); BBC News Staff Writer, “U.S. Major Contacted Radical Cleric,” BBC News, Nov. 10, 2009 available at http://news.bbc.co.uk/go/pr/fr/-/hi/americas/8351740.stm (noting that a “senior Republican” on the House Permanent Select Committee on Intelligence has called for intelligence agencies to preserve all information obtained on Hasan to facilitate a full committee review of the acquisition, interpretation and notification of relevant authorities).

Rucker, supra note 148 (reporting that Al-Aulaqi, a U.S. citizen who was previously an imam at a mosque in Falls Church, VA, operates a website from Yemen denouncing U.S. policy, particularly related to the ongoing conflicts in Afghanistan and Iraq).

See 50 U.S.C. §1804(a)(1)-(11); see also 50 U.S.C. §1881c(b)(3)(B) (requiring the same standards for surveillance of U.S. citizens reasonably believed to be outside the U.S.).

Given that Hasan was enlisted in the Army, it is unclear whether his messages were subject to greater scrutiny or monitoring than would be expected for a civilian. If the issue of why surveillance was authorized should arise in the ensuing investigations, that topic will likely be elucidated.


See id.


See id.

Id. (reporting that a consultation performed by the government to gauge public support returned only 29% positive reviews of the proposed measures, which are seen as an expansion of the already-controversial powers granted under RIPA).

DCAF Backgrounder, supra note 20, at 3.