SCOWCROFT INSTITUTE
OF INTERNATIONAL AFFAIRS

Scowcroft Paper No. 8

The Foreign Intelligence Surveillance Act of 1978 Compared with the Law of Electronic Surveillance in Europe

By Ronald J. Sievert, J.D.

Senior Lecturer at the Bush School of Government and Public Service and Director of the Certificate in Advanced International Affairs Program

February 2017

Paper commissioned by the Scowcroft Institute of International Affairs

For more information: bush.tamu.edu/Scowcroft/

The Bush School
OF GOVERNMENT & PUBLIC SERVICE
TEXAS A&M UNIVERSITY

*The Foreign Intelligence Surveillance Act of 1978 Compared with the Law of Electronic Surveillance in Europe**

By Ronald J. Sievert

Introduction

In the summer and fall of 2013 there were strong political, media, and public reactions to the disclosures of Edward Snowden regarding electronic surveillance conducted by the United States. These tended to create the impression of the U.S. government as ever present, snooping on every citizen's private actions and conversations. [1] As the author has pointed out in previous articles, the reality is that the law and procedures regulating U.S. domestic surveillance are highly restrictive.[2] In fact, notably absent from the furor surrounding the Snowden revelations were any verified claims of innocent citizens being harmed by U.S. surveillance.

The purpose of this article is to compare the fundamental operative provisions of the U.S. Foreign Intelligence Surveillance Act (FISA) with the equivalent directives of European surveillance law in five representative countries. The specific provisions being compared relate to the ability to monitor the content of individual communications within the nation state or citizens outside territorial borders. The author is not greatly concerned at this point with the procedure required before interceptions of non-citizens outside the country as under U.S. law this is not limited in a manner that endangers the nation. Foreign residents outside the country are not protected by the Fourth Amendment and thus there are less obstructive regulations.[3] Nor is there a need at this time to concentrate on metadata collection, which is simply the accumulation of data on numbers dialed, time, and duration of calls made by telephone subscribers. Metadata does not include content.[4] Although the provisions of the USA Freedom Act will increase the burden on the government by directing that this data be stored with the separate telecommunications providers instead of NSA,[5] the threat posed by these provisions is minor compared to the dangers created by the restraints of the FISA statute on the ability of the government to intercept citizens and communications domestically.

In this later area, an examination of European law will reveal that the authority provided to the Executive under less demanding standards than the U.S. and with reasonable oversight results in more efficient security procedures than the current U.S. regime while still fully complying with the strict guidelines established to protect privacy by the European Court of Human Rights.

The author's recent 2014 National Security Law Journal article on the creation of FISA contained a very brief review of European surveillance law.[6] As the core of that article was an analysis of FISA, the section on European law was "bare bones" to say the least. For the following analysis of current surveillance law in five major European countries, the author has had access to a number of important current studies. These include Winston Maxwell and Christopher Wolfe, *A Global Reality: Government Access to Data in the Cloud*,[7] Francesca Galli, *The Law on Terrorism: The U.K., France and Italy Compared*,[8] the Report of the European Union Agency for Fundamental Rights on Intelligence

* ***Paper commissioned by the Scowcroft Institute of International Affairs; the full article was first published in the American Journal of Criminal Law, vol. 43, number 2, Spring 2016, pp. 125-155.***

Surveillance,[9] the UN Office of Drug Control Report on Electronic Surveillance in Member Nations,[10] the ongoing work of the Library of Congress on Foreign Intelligence Gathering Laws,[11] Simon McKay's treatise on Covert Policing in the U.K,[12] and other articles cited throughout. All were helpful, although none provided in whole exactly what was being sought in terms of how surveillance worked practically in comparison with U.S. Law. Somewhat more helpful have been actual personal and electronic interviews, aided by funding from the Scowcroft Institute of International Affairs, with key practitioners and scholars including, among others, Ms. Galli, Mr. McKay, German Professor of Intelligence Law Jan-Hendrik Dietrich, Judge Doctor Markus Loffelman, and Professor Doctor Reinhard Klaushofer.

The first section of this article cites scholars, practitioners, and actual events to explain in detail exactly why the restrictive provisions of FISA endanger the security of the U.S. and why these rules are not required by the U.S. Constitution. It is the author's belief that a much more reasonable approach is needed to obtain surveillance of content in cases involving al Qaeda, ISIS, or the threat of WMD. The second section of this article will then review at length the comparable provisions guiding electronic surveillance of content in Germany, the United Kingdom, France, Italy, and Spain. The conclusion will highlight the important differences in the two systems and propose possible amendments for U.S. surveillance law.

FISA

In the United States, the Foreign Intelligence Surveillance Act (FISA) requires that the federal government prove to a designated federal judge "probable cause" that a US person or individual present in the US is "an agent of a foreign power" before conducting electronic surveillance to obtain the content of their communications.[13] This is the highest criterion in U.S. search law, beyond such other legitimate standards as relevance, reasonable suspicion and articulable suspicion.[14] The FISA statute was passed by the post-Watergate Congress in 1978, and based its provisions on the same probable cause standards that had been enacted in 1968 to justify interceptions in cases of ordinary crime.[15]

However, as stated by numerous courts both before and after the enactment of FISA, the criminal law probable cause standard is not constitutionally required for searches conducted to obtain intelligence information in national security cases.[16] Moreover, as will be explained following, the requirements of FISA have "created an unnecessarily protracted risk adverse process that is dominated by lawyers, not investigators and intelligence collectors"[17] that has arguably already endangered the safety of U.S. citizens in numerous reported terrorist cases.[18]

In the Supreme Court's landmark case of Katz v. U.S. holding that probable cause warrants were required in ordinary crime cases, Justice White stressed that:

> There are circumstances in which it is reasonable to search without a warrant. In this connection, ….the Court points out that today's decision does not reach national security cases. Wiretapping to protect the security of the Nation has been authorized by successive Presidents. [19]

The Court followed four years later with U.S. v. U.S. District Court relating to the need for a warrant in investigating wholly domestic groups "composed of citizens of the U.S. which (have) no significant connection with a foreign power,

its agents or agencies,"[20]as opposed to "the activities of foreign powers or their agents."[21] The Court then cited the American Bar Association's standards on electronic surveillance supporting "the view that…warrantless surveillance may be constitutional where foreign powers are involved." The Court's emphasis that it was not imposing a constitutional requirement of probable cause warrants approved by magistrates in foreign intelligence cases only naturally followed from reference to preceding legal and factual history including that in 1940 when President Roosevelt had authorized Attorney General Jackson to utilize wiretaps for national defense, Attorney General Tom Clark had advised President Truman of the necessity of such wiretaps,[22] and Attorney General Brownell had sanctioned their employment by President Eisenhower.[23]

In the years immediately following Keith, four separate federal circuit courts "readily accepted the existence of a foreign intelligence exception to the warrant requirement based on the legal and policy arguments put forth by the Executive."[24] Typical of the reasoning of these courts was the Third Circuit's en banc opinion in U.S. v. Butenko:

> In the present case, too, a strong public interest exists: the efficient operation of the Executive's foreign policy-making apparatus depends on a continuous flow of information. A court should be wary of interfering with this flow….Also, foreign intelligence gathering is a clandestine and highly unstructured activity, and the need for electronic surveillance often cannot be anticipated in advance. Certainly occasions arise when officers, acting under the President's authority, are seeking foreign intelligence information, where exigent circumstances would excuse a warrant. To demand that such officers be so sensitive to the nuances of complex situations that they must interrupt their activities and rush to the nearest available magistrate to seek a warrant would seriously fetter the Executive in the performance of his foreign affairs duties.[25]

Despite these cases, Congress, reflecting the distrust of the Executive in the Watergate era, passed FISA in 1978 imposing the same requirements of judicial approval and demonstration of probable cause on intelligence collection that it had ten years previously for ordinary crime. [26] This created the current bureaucratic risk-averse process that hinders intelligence collection.[27] Jimmy Carter was also the first President not to strongly oppose such restrictions.[28]

Although the Supreme Court has resisted efforts to define the phrase "probable cause" in terms of statistical percentage,[29] it should come as no surprise that practitioners have come to focus on the word "probable" as meaning "more likely than not," so that:

> For practical purposes probable cause exists when an officer has trustworthy information sufficient to make a reasonable person think it more likely than not that the proposed arrest or search is justified. In math terms this implies that the officer or magistrate is more than 50 percent certain that the suspect has committed the offense or that the items can be found in a particular place.[30]

FBI Director James Comey has even stated that for FISA and T-III applications the government generally goes "beyond probable cause" to

establish and maintain credibility with the courts.[31] It can take experienced lawyers more than a week to prepare the paperwork, and the documents "are like mortgage applications in their complexity."[32]

This FISA standard has created great difficulty in obtaining intelligence to defend the security of the United States. Terrorists and spies often operate in a loosely connected cell structure that can be hard to identify, they are well trained in avoiding detection, and their schemes can be quiet and nascent before suddenly erupting with devastating consequences. Attorney General Alberto Gonzales defended the administration's much criticized TSP warrantless surveillance program against al Qaeda suspects in the U.S. on the basis that the FBI needed more "speed and agility" in meeting the threat.[33] NSA Director Michael Hayden amplified this comment in noting that the FISA probable cause standard was "too onerous."[34] Director of National Intelligence Mike McConnell testified about the number of man hours required to do the paperwork for a FISA and stated that "the current statutory requirement to obtain a court order based on probable cause slows, and in some cases prevents altogether, the Government's efforts to conduct surveillance of communications it believes are significant to the national security."[35] In his opinion, this standard required "substantial expert resources towards preparing applications….(diverting them) from the job of analyzing collection results and finding new leads."[36]

Such comments are not new or confined to those attempting to defend executive branch actions. In 1982, Senator Malcom Wallop expressed the view that the "net effect of FISA has been to confuse intelligence gathering with criminal law" and that it is "nonsense" to attempt a formula for comprehensive surveillance of those who constitute a security threat.[37] Gerald Reimers wrote that FISA's "extraordinary procedures and high standards of proof result in unnecessary delay if not a bar" to intelligence investigations.[38] Scholar Kim Taipale has written that when information comes from computers that do not reflect who placed the calls or their exact content, but legitimately focus the attention of government, it is almost impossible to establish probable cause in the FISA context.[39] Federal Judge Richard Posner stated that FISA's requirement of probable cause is no help "when the desperate need is to find out who is a terrorist."[40] Although strongly criticizing the expansion of FISA to include broad generic surveillance operations, noted professor William C. Banks recently acknowledged that in ongoing counterterrorism investigations where it might be impractical to seek a warrant "it is no longer realistic to argue that the Warrant Clause and its traditional law enforcement warrants and the criminal law version of probable cause should apply in the foreign intelligence context."[41] In the words of one Wall Street Journal commentator, "one would think that agents charged with protecting us from a 'dirty nuke' would enjoy the same discretionary search authority as a patrolman who makes a traffic stop. In fact, they have less."[42]

As explained by numerous federal judges, the public claim that the FISA Court is somehow a rubber stamp because most applications are, in the end, approved, has no basis in fact and does not reflect the real difficulty of obtaining a FISA.[43] In the opinion of Judge Richard Posner, the positive statistics are a reflection of the fact that the government is actually far too conservative in seeking surveillance orders. He believes that in our legalistic culture the FBI tries to not only avoid violating the law but does not want to even sail close to the wind. "The analogy is to a person who has never missed a

plane in his life because he contrives always to arrive at the airport eight hours before the scheduled departure time."[44]

A DOJ internal report prior to 9/11 strongly suggested that FISA greatly hindered the FBI in the Wen Ho Lee and Aldrich Ames espionage investigations involving the transfer of enormously damaging national security information to our potential enemies.[45] Days before the 9/11 attacks the FBI had detained hijacker Zacarias Moussaoui in Minneapolis, but agents were prevented from scanning his computer because a supervisor at FBI Headquarters concluded there was not probable cause for a FISA warrant. Meanwhile, in the words of the DOJ Inspector General's report, the Minneapolis office believed that "probable cause for the warrant was clear" and "became increasingly frustrated with the responses and guidance it was receiving."[46] The government apparently knew that 2007 Times Square bomber Faisal Shazad had "established interaction with the Pakistani Taliban, including bomb-making training in Waziristan" and had made "thirteen trips to Pakistan in seven years," yet did not monitor him as he slowly assembled the materials to construct his potentially devastating weapon.[47] This led the *Wall Street Journal* to question whether this failure was due to "restrictions imposed on wiretapping by the Foreign Intelligence Surveillance Act" and quote officials on the reduced effectiveness and excessive delays of the judicially regulated program.[48] In a very extensive, detailed investigation of the Boston marathon bombing, Keith Maart further highlighted the constant confusion that is pervasive as reasonable people try to interpret FISA. He noted that, based on the facts that the Russian FSB had twice informed the FBI and CIA that Tamerlan Tsarnaev "had contacts with foreign Islamic militants/agents, was visiting jihadist websites, was looking to join jihadist groups" and had travelled to Dagestan on an unknown mission, it would certainly appear there was "sufficient probable cause to obtain FISA warrants that would allow…more encompassing surveillance." FBI lawyers had apparently come to a contrary conclusion.[49]

Since 2001, the FISA Court of Review has again echoed the opinions of the Appellate Courts prior to the enactment of FISA by noting that probable cause is simply not required by the Constitution for the collection of foreign intelligence. The Fourth Amendment states that:

> 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.[50]

In the words of Chief Justice Roberts, "As the text makes clear, 'the ultimate touchstone of the Fourth Amendment is reasonableness.'"[51] That is, although the Fourth Amendment states that warrants should be supported by probable cause, the ultimate test of the Constitutionality of a search is whether it is reasonable, not whether the government has established probable cause. Noted Constitutional Law scholar Reed Akhil Amar has written that those who seek to impose a "global probable cause requirement have yet to identify even a single early case, treatise, or state constitution that explicitly proclaims "probable cause" as the prerequisite for all "searches and seizures."[52]Over the past 50 years the Supreme Court has repeatedly sanctioned searches without probable cause in "special circumstances" where significant safety and security concerns were present. These cases

involved, among others, regulation of the catering and liquor industry,[53] firearms sales[54] and enforcement of city housing[55] and occupational safety codes[56]

The FISA Appellate Court of Review suggested the applicability of these cases when it approved FISA Patriot Act amendments in In Re Sealed Case.[57] The court noted that the "threat to society…certainly remains a crucial factor" in determining whether a particular search is "reasonable" under the Constitution. It cited the Supreme Court's approval of "warrantless and even suspicionless searches that are designed to serve the government's special needs beyond the normal need of law enforcement."[58] The court further referenced the "president's inherent constitutional authority to conduct warrantless foreign intelligence surveillance."[59]

In 2008, the FISA Court of Review clearly acknowledged the applicability of the above cited special needs cases in the domestic FISA context with its decision in In Re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act.[60] The case involved an appeal by the service provider of a FISA court finding that it was constitutional for the Attorney General to direct the interception of the communications of a U.S. person located outside the U.S. At the time, this was authorized without a FISA court order pursuant to the Protect America Act of 2007 (PAA).[61] However, one year later Congress passed the FISA Amendments Act (FAA), [62] requiring a FISA Court order when surveillance was directed against U.S. persons even if they were located outside the US. Analyzing the previous PAA, the FISA review court expressly found what had been hinted at by In Re Sealed Case[63]; that is, there is a "foreign intelligence exception" to the probable cause judicial warrant requirement. In the FISA review court's opinion,

> The (Supreme Court) has recognized a comparable exception, outside the foreign intelligence context, in so-called 'special needs' cases. In those cases, the Court excused compliance with the Warrant Clause when the purpose behind the governmental action went beyond routine law enforcement and insisting upon a warrant would materially interfere with the accomplishment of that purpose."[64]

The FISA review court further found that "here the relevant government interest -- the government's interest in national security -- was of the highest order of magnitude."[65] Individual privacy rights, on the other hand, were protected by executive branch findings, certifications and minimization requirements restricting the distribution of the information. The surveillance of U.S. persons without judicial warrant therefore met the key "reasonableness" test of the Fourth Amendment. It was only Congress, through FISA, and the FAA, that imposed greater restrictions.

Electronic Surveillance in Europe

Numerous legal commentators have written quite favorably about the European approach to privacy protection as opposed to what they consider more intrusive U.S. laws.[66] In their opinion, "The U.S. Constitutional amendment protections (as applied) and U.S. federal and state laws fall short" of international standards.[67] The European convention with the enforcement mechanisms embodied by the European Court of Human Rights are considered to form the "most comprehensive and effective system for the protection of human rights in the world"[68] As might be expected, in Europe there was loud and public (if disingenuous) fury over what some believed to be Edward Snowden's "monstrous

allegations of total monitoring of various telecommunications and internet services."[69]

Yet, according to a study by the Max Planck Institute quoted by Stewart Baker, "you are 100 times more likely to be surveilled by your own government if you live in the Netherlands or if you live in Italy…[and] 30 to 50 times more likely to be surveilled if you're a French or German national then in the United States." [70] Relevant to this article is the fact that in national security matters, most of the major European powers, unlike the U.S., **do not require either judicial approval or a standard close to probable cause** before the government with general legislative oversight can conduct electronic surveillance to protect national security.[71] Indeed, when a magistrate is involved in the process it is almost always an investigating magistrate as opposed to a neutral, non-participating judge in the mold of the American judiciary. The content of interceptions is often, but not always, admissible in court.

All governmental surveillance in Europe must comply with Article 8 of the European Convention on the Protection of Human Rights.[72]Article 8 provides that:

Right to respect for private and family life.

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

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.[73]

European States thus enjoy discretion in enacting surveillance provisions, but they must comply with Article 8 as interpreted by various cases of the European Court of Human Rights. Measures have to be in accordance with established law, have a legitimate aim, such as national security, safety and "economic well-being," be necessary in a democratic society, and be proportionate. "Proportionate" refers to the fact that the invasion of privacy is justified by the need for the information. As stated by Professor Francesca Galli, "A crucial factor for proportionality is the existence of sufficient safeguards to ensure that the measures are not carried out in an excessive or arbitrary manner … Surveillance techniques must represent the *extrema ratio* and only be permissible if the establishment of the facts by any other method is without prospects of success or considerably more difficult."[74] This is reflected in most European statutes and is mirrored in Title III of the U.S. Code on electronic surveillance requiring a statement as to why other investigative procedures "reasonably appear to be unlikely to succeed if tried or to be too dangerous."[75]

The European Court further requires that surveillance law must be clear, predictable and meet a minimum set of safeguards, as summarized in the 1996 landmark case of Weber and Savaria v. Germany:

> [F]oreseeability in the special context of secret measures of surveillance, such as the interception of communications, cannot mean that an individual should be able to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly […]. However, especially where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident […]. It is

> therefore essential to have clear, detailed rules on interception of telephone conversations, especially as the technology available for use is continually becoming more sophisticated […]. The domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures […]. Moreover, since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive or to a judge to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference.[76]

With regards to safeguards, the Court stated:

> In its case-law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in statute law to avoid abuses of power: the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed.[77]

With this introduction, the following explains the specific provisions for electronic surveillance in Germany, the U.K, France, Italy and Spain.

Germany

The Basic Law of the Federal Republic of Germany provides that:

> 1. The privacy of correspondence, posts, and telecommunications shall be inviolable.
> 2. Restrictions (exemptions) may only be ordered pursuant to a law. If the restriction serves to protect the free democratic order or the existence or the security of the federation…the law may provide that the…recourse to the courts shall be replaced by a review of the case by bodies and auxiliary bodies appointed by parliament.[78]

Germany, as most of the European governments that will be reviewed, attempts to maintain a "strict separation between the task of the police to fend off threats and to prosecute crimes on the one hand and the collection of information carried out by the intelligence services on the other."[79] In criminal cases involving listed crimes, surveillance for a lengthy period currently may only be authorized by an investigating judge after the police and prosecutor submit an application demonstrating reasons for the surveillance. If the law is not followed, a judge may exclude the evidence obtained.[80]

In intelligence collection matters, applications must be made by the Federal or State Office for

the Protection of the Constitution (OPC), the Military Counter Intelligence Service Office (CI), or the Federal Intelligence Service (BND) first to their respective ministries. This is generally the Ministry of the Interior for OPC, Defense for CI and direct to the responsible Chancellery officials for BND.[81] These ministry departments were formerly coordinated by an executive branch Commissioner for Intelligence Services, which the Chancellor recently designated as the Secretary of State for Intelligence Service Issues.[82] Applications must be in writing and demonstrate to the ministry and G-10 Commission that "concrete indications give rise to the suspicion that a person is planning, committing or has committed" significant listed crimes against state security.[83] They should also establish that "the use of another method to investigate the facts would be futile or render the investigation significantly more difficult,"[84] and should not intrude upon a "core area of the private sphere."[85]

The relevant ministry may then issue an order for the interception which must be in writing "state the grounds for the order and the agency authorized to carry out the monitoring and the nature, scope and duration" of the interception.[86] Outside of emergency situations, however, the order must be approved by the G-10 commission before it can be executed.[87] The commission, comprised of a chair person who is a legal expert, three associate chairpersons and four deputies, meets once a month to decide whether the interception is "permissible and necessary"[88] and meets the stated standards. It is the only expert body other than the ministry which reviews the interception before it is initiated.

The G-10 commission is appointed by a Parliamentary Control Panel which appears to be a "mainstay of legislative control."[89] This body consists of nine members of parliament who also only meet once a month, but have the power to inspect all files of the intelligence services, visit facilities, and question staff members.[90] They may issue reports to the legislature and "assess certain intelligence activities and publish such an assessment, provided this is in keeping with confidentiality regulations."[91] However, "their main task is to be a member of Parliament and not an inspector of intelligence services."[92]

As is the case of intelligence surveillance in most of the European nations examined, judicial review is not required for the Executive to initiate an interception. The European Court of Human Rights upheld this principle in the case of Klass v. Germany. The court held that judicial consent was not necessary and that other safeguards were sufficient, as long as these were independent and vested with powers to exercise effective and continuous control.[93]

This does not mean that the courts never have an opportunity to review surveillance. The data may be transferred to the prosecutor where "concrete indications give rise to the suspicion of planned or completed offenses and this evidence may be used in court.[94] The ability to utilize the information in court, subject to protection of sources and methods, is the norm in the countries examined, with the exception of the UK. In addition, although targets of surveillance are of course not notified at the time of the interception, they must be informed as quickly as possible once disclosure no longer impedes the fulfillment of the government's mission, leading to the possibility that the targets may seek recourse in the German courts.

Germany does not require that the procedures listed above be followed for security surveillance conducted outside the country. This is consistent with the U.S. principle announced in U.S. v. Verdugo-Urquidez to the effect that our Constitution does not apply to non-citizens overseas.[95] However, several German jurists

have presented arguments to Parliament suggesting that failure to comply with the above list of domestic procedures even when conducting surveillance in a foreign nation would be a violation of their basic law or Constitution.[96] As of the date of this writing, this matter was a subject of intense debate, but the German law had not changed.[97]

United Kingdom

The U.K, like other European countries, long had an unstructured system of electronic surveillance which was eventually castigated by the European Court of Human Rights.[98] The result was the 2000 passage of the Regulatory of Investigatory Powers Act (RIPA).[99] As stated by Simon McKay in his book, *Covert Policing*, RIPA is a landmark piece of legislation regulating surveillance for the first time in the UK and including specific provisions for the interception of communications on private communications systems. In addition, Codes of Practice are regularly issued to guide surveillance and electronic interception activities.[100] In 2010, the European Court of Human Rights found that RIPA was in compliance with Article 8 privacy requirements with its holding in Kennedy v. United Kingdom.[101] Pursuant to RIPA, as is the case with other European nations, the judiciary is not generally involved in security surveillance. However, unlike many other nations, in the UK it is a general rule the product of that surveillance cannot be used in court.[102]

Section 5 of RIPA provides that the relevant Secretary of State (often the Home Secretary in domestic matters) can issue an intercept warrant if he believes it would be "necessary in the interests of national security, for the purpose of preventing or detecting serious crime, for the purpose of safeguarding the economic well-being of the United Kingdom, or for the purpose of giving effect to the provisions of international mutual assistance agreements."[103] The standard, as set forth in RIPA and the Code of Practice, is that the Secretary of State must determine whether the interception is necessary, whether the information can be reasonably obtained by other means, and whether the interception requested is proportionate to what is sought to be achieved. That latter concept has been explained above by the ECtHR.[104]

There are only a limited number of persons authorized to apply to the Secretary for a warrant, and these include the Director General of the Security Service (MI 5), the Chief of the Secret Intelligence Service (MI6), and Chief Constables.[105] The application, and subsequently the warrant, will detail the operational background, a description of the targeted person or premises, and the types of communications that are likely to be intercepted.[106]

The content of the interceptions must be destroyed once they are no longer needed for the authorized purposes.[107] As defined, the phrase "authorized purposes" does not include use by the prosecutor as evidence in trial or review by a criminal defense attorney. [108] McKay acknowledges that "it is this latest provision that is the most problematic and where tensions have arisen."[109] In the words of Francesca Galli, "the intelligence services and many sections of the police are particularly keen to prevent disclosure of any intercept evidence to the public on the grounds that it would spoil the efficacy of this investigative technique by alerting suspects of their sources, methods and interception capabilities, which allow them to prevent and disrupt terrorist outrages and serious crimes."[110] She notes, however, that some suggest these security concerns really mask the unwillingness of the Secretary of State and law enforcement to have the lawfulness and proportionality of intercepts scrutinized by the courts.[111]

Apparently there have been "eight reports in the last thirteen years to government ministries on this issue." [112] Many of these reports, as well as government officials, have come out in favor of the admissibility of intercept evidence in criminal trials.[113]

However, section 18 of RIPA does provide for the disclosure of intercept material to the prosecutor so that he can decide whether a prosecution should continue consistent with the duty to see that justice is done in a fair manner. It may also be given to a judge "in the interests of justice" or to determine whether certain facts should be admitted at trial.[114] There are also exceptions permitting disclosure for proceedings involving a violation of the Act itself, before the Investigatory Powers Tribunal or the Special Immigration Appeals Commission.[115]

Parliamentary control is theoretically provided through the Intelligence and Security Committee which is charged with overseeing the expenditure, administration, policy and operations of the security and intelligence services. However, this committee cannot review particular operations or ongoing matters unless requested by the Prime Minister or a government department.[116] Scrutiny of the functions of the intelligence services is instead provided by a number of executive bodies including the Interception of Communications Commissioner (ICC), the Intelligence Services Commissioner (ISC), the Chief Surveillance Commissioner CSC) and the Investigatory Powers Tribunal (IPT). [117]

Determining the exact roles of these officers, and where they overlap, is sometimes difficult based on a simple reading of their duties. In essence, the ICC is an individual qualified as a high judicial official who does not perform a judicial function but rather is responsible to "keep under review" the performance of the Secretary of State with respect to acquisition and disclosure of intercepted material. He cannot order that a warrant be quashed or content be destroyed, but he may report to the Prime Minister or IPT.[118] The ISC must "keep under review the carrying out of any functions of the intelligence services, a head of an intelligence service, or any part of Her Majesty's Forces, or the Ministry of Defense, so far as engaging in intelligence activity."[119] In all other respects, "the functions and duties of the ISC are in the same terms as those relating to the ICC."[120] The Chief Surveillance Commissioner must actually approve all warrants to enter property used as a dwelling, hotel bedroom or office. [121] The Chief shall also keep under review the performance of personnel conducting surveillance activities "insofar as they are not required to be kept under review by the ICC and ISC."[122] Finally, the Investigatory Powers Tribunal (IPT) has fairly broad jurisdiction to investigate complaints against powers granted under RIPA. It has the power to investigate any alleged violation of human rights that may have occurred under RIPA and whether any conduct was justified and proportional.[123] The hypothetical power of the IPT is offset by the fact that the absence of disclosure of surveillance activities "means that the majority of interferences with privacy will be undetected."[124] Disclosing the existence of a warrant would be an offense under section 17 of RIPA, although it is always possible that violations may become public pursuant to the disclosure exceptions noted above.

As of this writing there is a proposal pending in Parliament to create a body of separate judicial commissioners under an Investigatory Powers Commissioner to review surveillance applications. [125]This new system, however, would not approximate the independent judicial review that those in the civil liberties community have been demanding. The Commissioners

would apparently be charged with simply ensuring proper procedures were followed instead of reviewing the evidence de novo. In addition, they would be appointed by the government only, without vetting by the Parliament or judiciary, and they could be removed after three years.[126] The overall power to intercept electronic communications would thus apparently still rest firmly in the hands of the Executive branch with quite limited oversight.

France

The French Code of Domestic Security provides that "the secrecy of correspondence emitted via electronic communications is guaranteed by law,"[127] but that there may be exceptions for national security or essential elements of the scientific and economic potential of France.[128]

Prior to 1991, the French electronic surveillance regime was essentially built upon case law and ad hoc procedures without a solid statutory framework.[129] As might be expected, the European Court of Human Rights found that this practice did not comply with Article 8's requirement that interference with private communications be grounded upon established legal provisions.[130] In response, France passed in 1991 its foundational law 646/91 on the Secrecy of Communications Issued by the Telecommunications Channel.[131] This was followed by a series of amendments relating to interceptions in criminal cases,[132] counter terrorism, and national security matters.[133] The ECHR has found the practice established by these statutes to be in compliance with Article 8.[134]

Pursuant to the statutory framework of 646/91, the French Code of Criminal Procedure incorporated detailed provisions specifying when courts and prosecutors could intercept conversations.[135] A Juge d'instruction is a judge of inquiry who is tasked with determining whether sufficient evidence exists to proceed to a criminal trial, generally with reference to completed crimes. This judge may order an interception as part of his general evidence-gathering powers. However, this type of interception is not necessarily routine, as one of the key principles of 646/91 applying to all French wiretaps is that they should only be initiated in extrema ratio or where other investigative methods would be unsuccessful or unavailable.[136] This basic language is very similar to that quoted above as required by the ECtHR.

The French Government recognized it needed some active method of interception for ongoing crimes (in flagrante) and in 2004 passed law 204/2004 noting that in a limited number of listed serious crimes, such as those committed as part of organized crime, a juge des liberties et de la detention, or judge of liberty and detention, could order a wiretap upon application of a prosecutor. The standard would be the same as above. Apparently the police and prosecutor can begin the surveillance and send the application to the court to obtain permission retrospectively.[137]

All the evidence obtained in these interceptions is admissible in court. [138] This is consistent with other European jurisdictions but contrary to English law. [139] It should be noted that, with respect to the retrospective approvals requested from the judges of liberty and detention, it would be expected that an application that did not meet required standards would probably result in the suppression of the evidence. Thus, there is certainly motivation for the police and prosecutors to submit an application that complies with the law even if they start surveillance before obtaining judicial consent.

In national security cases which can include the protection of French scientific and economic resources, prevention of organized crime and terrorism, Law 646/91 Articles 3-19 permit the prime minister, upon application of the Defense, Customs or Interior Ministers, to order an interception without permission from the courts.[140] This practice has been continued with the 2012 decree of a Code de la Securite Interiure, or Code of Homeland Security, designed as a compilation of the pertinent sections of French national security law.[141] The standard is a "written and reasoned warrant "upon "a written and reasoned application."[142] The only timely review is conducted by the Commission nationals de controls des interceptions securite (CNCIS),[143] recently renamed the National Commission for Control of Intelligence Techniques (CNCTR).[144] The CNCTR is composed of nine members: two representatives of the National Assembly, two Senators, two members of the Council of State, two judges of the Court of Cassation, and one associate with skills in electronic communication. The Commission assesses whether prescribed procedures are followed, and whether these respect the right to privacy and the principle of proportionality. Should the CNCTR consider a surveillance measure to be carried out unlawfully, it can recommend to the prime minister, the relevant minister and the intelligence service that the surveillance be interrupted and the collected data destroyed. The prime minister must immediately inform the CNCTR about how the recommendation was followed, but recommendations are not automatically enforced.[145] Negative recommendations appear to be rare.[146] Among its other duties, this body ensures that recording and duration procedures are followed. It can also review cases filed by individuals claiming a violation of statutory provisions.[147]

The contents of security interceptions, being preventive in nature, are supposed to be erased at the end of the operation.[148] Accordingly, the content is not normally admissible in a criminal trial. However, where major criminality is discovered, the government can hand "the file" over to the criminal prosecutor, who then may initiate one of the previous mentioned judicial interceptions.[149] It is unclear how much of the contents of the security interception is contained in the file that is submitted to the courts to initiate a follow up judicial interception.

A review of the surveillance procedures in the major European nations, as indicated above in France, reveals that the executive branch makes the relevant operational decisions with little direct interference from the judiciary or legislature. However, some degree of at least general oversight is occasionally provided by parliamentary committees or expert bodies.[150] In France, legislative oversight is accomplished through the parliamentary intelligence delegation (*délégation parlementaire au renseignement*, DPR). This body examines and assesses governmental policy in the area of intelligence but does not oversee the services directly. It does not have access to information about ongoing operations carried out by the services or surveillance methods or information regarding exchanges with foreign services. [151] The DPR may conduct hearings and request reports, and can make recommendations to the president of the republic and the prime minister. Requests for classified documents from parliamentary committees tend to be rejected, and members of parliament have no right to hear or question members of the intelligence services.[152]

There are ongoing criticisms by the civil liberties community of the French system. One related the lack of judges on the CNCIS,[153] but this was remedied to an extent with the inclusion

of two judges on the CNCTR. Still, the CNCTR can only make non-binding recommendations. Other complaints target the broad definition of national security and the fact that there is no statutory maximum number of renewals for security interceptions.[154] As of this writing there have been no changes in these areas.

Italy

In Italy, Article 266 et seq of the Codice di Procedura Penale, or Code of Criminal Procedure, allows a prosecutor to apply to a judge for an interception warrant when investigating the commission of an offense that has already taken place.[155] The offense must be a serious offense involving a penalty greater than five years such as the use of drugs, firearms or explosives.[156] The judge will approve the interception based on "a reasoned decision where there are serious grounds for believing that a crime has been committed and it is absolutely indispensable for the purposes of the investigation."[157] The judge clearly must be provided enough evidence to support a "reasoned decision," but apparently he does not get access to the full file. [158]

In organized crime, human trafficking and terrorism cases, where there is an established investigation, the judge may authorize an interception with somewhat less stringent standards. Specifically, there need only be "sufficient grounds" as opposed to "serious grounds," and the interception need only be "necessary" instead of "indispensable."[159] The results of the interception may also be used to expand into other investigative areas.

The contents of both these types of interception are admissible in court. However, if proper procedures are not followed, the contents may be suppressed.[160] If the content reveals state secrets, the government or the court may decide to withhold the content.[161] This is similar to the practice with the Classified Information Procedures Act in The US.[162]

These interceptions apply to established investigations of crimes already committed. From a standpoint of security, there are procedures for preventive interceptions in organized crime and terrorism cases contained in Article 5 of 438/2001.[163] The courts are not involved in these interceptions. Rather the Minister of the Interior[164] or the Agenzia Informazioni e Sicurrezza Esterna (AISE) or internal (AISI) acting under the Prime Minister may apply for an interception warrant. A warrant will be issued by the prosecutor if, based on the evidence shown, it is "deemed to be necessary to prevent terrorist activities or subversion of the constitutional order,"[165] to "protect the independence, integrity and security of the Republic . . . against threats originating abroad," or to preserve "Italy's political, military, economic, scientific, industrial interests."[166] This information cannot be used as evidence in criminal trial.[167] However, when a criminal violation becomes manifest, the file may be transferred to a public prosecutor who may then apply to the court to start a subsequent criminal investigation.[168]

In Italy there are no expert bodies like the CNCTR that review government electronic surveillance, although a Garante or Data Protection Authority has been established to "protect fundamental rights and freedoms in connection with the processing of personal data." [169] Parliamentary oversight is provided by the Committee for the Security of the Republic (COPASIR).[170] The Intelligence services are supposed to report the requests that have been made for wiretapping to the committee, and the committee members may inspect the various organizations that make up the Intelligence Community. COPASIR may order the

government to conduct internal investigations if it suspects illegal action.

There have been a number of complaints in Italy about the press obtaining the contents of intercepted communications even before the conclusion of a preliminary investigation. There has also been a proposal to change the standard for criminal interceptions from "reasoned decision" to "evident suspicions of guilt," but apparently this was abandoned by the government in 2011.[171]

Spain

Article 18.3 of the Spanish Constitution provides that communications, particularly postal, telegraphic and telephone communications shall be confidential unless a court decides otherwise.[172] Article 579 of the Spanish Code of Criminal Procedure provided that a Judge can issue a warrant if there is evidence that facts and circumstances material to a case could be uncovered. This was also used previously by the intelligence services.[173] The European Court of Human Rights found these procedures to lack of clarity and foreseeability. [174]The Spanish Constitutional Court has since established rules that appear to comply with the ECtHR, especially with respect to new procedures requiring "sufficient justification to restrict the fundamental right of communication," and respect to proportionality so that a judge may cease interceptions when it is no longer necessary to interfere with an individual's rights.[175] The standard appears to be "evidence that a relevant issue or circumstance of the case may be discovered."[176]

There was no clear legal framework regulating the surveillance activities of the Spanish Intelligence Services prior to 2002.[177] In 2002, the Parliament passed the National Intelligence Center Act,[178] designating the Center as the agency in charge of collecting and analyzing information to "promote the political, economic, industrial, commercial and strategic interests of Spain."[179] This includes avoiding threats and attacks on the independence of the state, its territory and the rule of law.[180] To achieve these goals, the Center was empowered to "collect and interpret signals intelligence."[181] The NIC is supervised by a Secretary of State-Director of the National Intelligence Center who reports to a Government Delegate Commission for Intelligence Affairs under the authority of the Prime Minister. The legislature has a standing committee on Intelligence Affairs or Official Secrets Committee that monitors intelligence spending[182] and is to receive "appropriate information about the functioning and activities of the NIC."[183] At the same time as the NIC was created, Parliament also passed the Act on Judicial Oversight of the National Intelligence Center.[184]

The Judicial Oversight Act provides that before an interception can be initiated in an intelligence case the office of the Secretary of State-Director of Intelligence must apply to a judge for a warrant.[185] The Judge is a member of the Supreme Court appointed for a five year term and his decisions must remain secret.[186] The government's application must state the nature of the investigation, the reasons for an interception, who would be affected, and the likely duration and locations of electronic surveillance.[187] In accordance with the prior cited case law, the standards would presumably be "sufficient justification" and "proportionality," although the Judicial Oversight Act does not provide that the judge actually supervise the monitoring of communication. The Act also does not contain provisions for notifying targeted parties even when notification would no longer interfere with the investigation.

In addition, In cases of urgency, when investigations are carried out to uncover felonies related to the acts of armed gangs, terrorist elements or rebels, the interception of communications may be ordered by the Minister of Home Affairs, or otherwise, the Director of State Security. They must communicate this order immediately by a "reasoned opinion" in writing to the relevant judge, who will also by a reasoned opinion, revoke or confirm such resolution in a maximum term of 72 hours.[188] If Parliament declares a "state of alarm, emergency or siege" that is implemented by decree of the cabinet, Article 18.3 of the Spanish Constitution may be suspended and the government may intercept any kind of communications, provided that the interception is "necessary to clarify alleged criminal offenses or to maintain public order."[189]

Conclusion

There are two major points of difference that emerge when contrasting the cited European surveillance law with FISA. First is the fact that, with the exception of Spain, the judiciary is not involved in decisions on intelligence collection. Second is that none of the countries listed hold the government to as high a standard as probable cause before surveillance to protect the country may be authorized.

There have been numerous proposals to insert the judiciary into the intelligence collection process in Europe, but to date, these have not been adopted.[190] Objections relate to the highly technical and nuanced nature of intelligence matters which is beyond the scope of most judges.[191] Chief Burger made similar comments in CIA v. Sims,[192] noting that judges have "little or no background in the delicate business of intelligence gathering"[193] and that "what may seem trivial to the uninformed may appear of great moment to one who has a broad view of the scene and who may put…information in its proper context."[194] The British Home Secretary has responded to Civil Liberties organizations that interceptions of communications and such intrusions of privacy should be authorized by the Executive as someone who is accountable by election directly to the British people and who has a greater understanding of the wider context.[195]As previously indicated, in the landmark case 1978 case of Klass v. Germany, the European Court of Human Rights found that "the exclusion of judicial control does not exceed the limits of what may be deemed necessary in a democratic society."[196]

Of course, in criminal matters, most of the European nations do involve the prosecutor and a judge. This judge, however, is often an investigating judge whose duties are closely associated with a U.S. prosecutor investigating a case while adhering to his professional commitment to see that justice is done. They are not the same as U.S. trial and appellate judges. Still, a neutral judge is different than a government minister or the police. In that context, it is interesting to note that the European system did not set up the wall between law enforcement and intelligence that was established in the U.S. on the unsound basis that there were slight differences between Title III criminal interception and FISA intelligence interception.[197] With the exception of the U.K., the European nations had established procedures to share the intelligence take with law enforcement and to admit the evidence, sometimes redacted, in criminal court. This only makes sense as terrorism, espionage, sabotage and other crimes are at the same time subjects of intelligence collection and criminal prosecution.

Regardless, judicial approval in the U.S. may not be the major problem faced by the government, because by establishing a FISA Court we have ensured that the judges reviewing

intelligence applications will over time have at least some understanding of intelligence matters. The greater concern is the burdensome standard that must be met before surveillance can be legally authorized in the U.S. Both Europe and the U.S. require extrema ratio, or evidence that other methods are unlikely to succeed or are dangerous. But the U.S. in addition demands an evidentiary affidavit showing to the judge demonstrating probable cause, or that it is "more likely than not" that a target is an agent of a foreign power before the government can legally proceed. A close review of the European law quoted verbatim above finds nothing close to such a high standard. The phrases used in the European statutes and court cases are "concrete indications giving rise to suspicion," "permissible and necessary," (Germany)"necessary and proportionate" (U.K.), "written and reasoned warrant," (France),"reasoned decision," "sufficient grounds," (Italy) "sufficient justification" and "evidence that material facts may be discovered" (Spain). All suggest that the government cannot conduct surveillance without good reason, but none of these imply that the government must wait to get enough evidence to be able to demonstrate to a court anything that could be interpreted as it being "more likely than not" that a target is an agent of a foreign power at the time surveillance is initiated. None creates, as does FISA, "an unnecessarily protracted risk-averse process that is dominated by lawyers, not investigators and intelligence collectors"[198] that has arguably already endangered the safety of U.S. citizens in numerous reported terrorist cases.[199] The cited European law is "designed to be preventative in nature," discovering plots in the planning stages before it may be too late to thwart an attack.[200] Yet all of these laws still comply with "the most comprehensive and effective system for the protection of human rights in the world" as enforced by the European Court of Human Rights.[201]

As explained earlier in this article, the provisions of FISA are not mandated by the Constitution. They are also not required to reasonably protect privacy and human rights as reflected in decisions of the European Court of Human Rights. The statute is an unnecessary obstacle placed upon the government by the 1978 Congress before the advent of al Qaeda and ISIS. In matters involving members of those organizations, who are by any definition at war with the U.S., or cases involving a potential WMD, Congress should lower the standard for surveillance in line with the standards followed by our European allies.

The views expressed in this report are those of the author, and do not necessarily reflect the positions of any of the institutions to which he is affiliated, the Scowcroft Institute of International Affairs, the Bush School of Government and Public Service, or Texas A&M University.

References

[1] See e.g. Christian Science Monitor, NSA Revelations, A Timeline of What's Come Out Since Snowden Leaks Began, http://www.csmonitor.com/USA/2013/1016/NSA-revelations-A-timeline-of-what-s-come-out-since-Snowden-leaks-began/June-5-8-2013, Jim Newell, Thousands Gather in Washington in Anti-NSA 'Stop Watching US' Rally, The Guardian, October 26th, 2013, http://www.the guardian.com/world/2013

[2] Ronald Sievert, Patriot 2005-2007, Truth, Controversy and Consequences, vol. 11Texas Review of Law and Politics p.319 (2007), A New Perspective on National Security Law Policies During the Bush Administration, vol. 7 Rutgers Journal of Law and Public Policy 35 (2009), Time to Rewrite the Ill Conceived and Dangerous Foreign Intelligence Surveillance Act of 1978, vol. 3 National Security Law Journal 47, 2014.

[3] See warrantless surveillance authorized by the President Foreign Intelligence Surveillance Act 50 USC 1801 and 1802. See also U.S. v. Verdugo-Urquidez 494 U.S. 259 (1990).

[4] See Klayman v. Obama, 2013 WL 6598728, December 16th, 2013 and ACLU v. Clapper 959 F.Supp 2d 724, December 27th, 2013 for descriptions of metadata program.

[5] Public Law 114-23 (2015).

[6] Supra note 2

[7] Winston Maxwell and Christopher Wolf, A Global Reality: Government Access to Data in the Cloud, A Logan Lovell's White Paper, May 23, 2012 http://www.hldataprotection.com/2012/05/articles/international-eu-privacy/hogan-lovells-white-paper-on-governmental-access-to-data-in-the-cloud-debunks-faulty-assumption-that-us-access-is-unique/ and the following white paper by Maxwell and Wolf, A Sober Look at National Security Access to Data in the Cloud, May 22, 2013 http://www.hldataprotection.com/2013/05/articles/international-eu-privacy/white-paper-cloud-national-security and Privacy International https:''www.privacyinternational.org/reports//surveillance-policies.

[8] Francesca Galli, The Law on Terrorism: The UK, France and Italy Compared, Bruylant, Belgium (2015)

[9] Report of the European Union Agency for Fundamental Rights, Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU, 2015 at 19.

[10] United Nations Office of Drug Control Current Practices in Electronic Surveillance for Serious and Organized Crime

[11] Library of Congress, Foreign Intelligence Gathering Laws, 2014, https://www.loc.gov/law/help/foreign-intelligence-gathering/index.php

[12] Simon McKay, Covert Policing, Oxford Press 2015

[13] 50 USC section 1801-1805.

[14] The government can obtain a targets phone, financial, medical and other records pursuant to a Grand Jury subpoena or court order if the records are relevant to a federal investigation. Rule 17 (c)(1) FRCP, 50 USC 1861 (d). Police may stop a vehicle and do a frisk of the person based on "articulable suspicion." Terry v. Ohio 392 US 1, 30 (1968)

[15] Omnibus Crime Control and Safety Acts of 1968, Pub. L. N0. 90-351, title III, 18 USC 2518.

[16] See cases cited following.

[17] New York City Police Commissioner Raymond Kelly cited in Wall Street Journal, Surveillance and Shazad, Are Wiretap Limits Making it Harder to Discover and Pre-empt Jihadists. http://online.wsj.com/news/articles/SB10001424052748704250104575523844418292496.

[18] See following.

[19] Katz v. U.S. 389 U.S. 347 (1967) at 363.

[20] U.S. v. U.S. District Court (Keith) 407 U.S. 297 (1972) at 316 n.8

[21] Id. At 322

[22] Id. At 311 FN 10

[23] Id. At 311

[24] Americo Cinquegrana, The Walls and Wires Have Ears: The Background and First Ten Years of the Foreign Intelligence Surveillance Act, 137 U. Pa. L. Rev. 793, 804 citing U.S. v. Brown 484 F.2d 418 (5th Cir.1973), U.S. v. Buck 548 F.2d 871 (Ninth Cir. 1977), U.S. v. Truong 629 F.2d 908 (Fourth Cir. 1980), U.S. v. Butenko 494 F.2d 593 (3rd Cir. 1974).

[25] Id. At 605.

[26] See Cinquegrana, The Background and First Ten Years of FISA, supra note 12 at 806.

[27] Kelly supra note 17.

[28] Senator Birch Bayh, Hearing on Foreign Intelligence Surveillance Act of 1978, Hearing on S. 1566 Senate Select Committee on Intelligence, Subcommittee on Intelligence and the Rights of Americans, 95th Congress, 2d Sess, July 19th, 1978 page 3.

[29]Illinois v. Gates, 462 U.S. 213 (1983) at 237.

[30] Rolando Del Carmen, Criminal Procedure Law and Practice, Cengage Learning, January 1st, 2013, at 68, 69. See also Arlen Spector questioning government attorney on FISA: Q: What is the legal standard for probable cause……A. More probable than not. Q. Are you familiar with Gates v. Illinois? A. No sir. FBI Oversight in the 107th Congress by the Senate Judiciary Committee: FISA Implementation Failures, available at ttp://specter.senate.gov/files/specterspeaks?ACF6.pdf, reprinted in 149 Cong. Rec.4534

[31] James Comey, Address to the Yale Law School Criminal Investigations Class, April 25th, 2003, quoted in Nola Breglio, Yale Law Journal, Leaving FISA Behind; The Need to Return to Warrantless Intelligence Surveillance, 113 Yale L.J. 179.

[32] Richard Lacayo, Has Bush Gone Too Far. The President's Secret Directive to Let the NSA Snoop Without Warrants Sets Off a Furor, Time, Jan.9th, 2006.

[33] Alberto R. Gonzales, Att'y Gen., Prepared Remarks for Attorney General Alberto R. Gonzales at the Georgetown University Law Center (Jan. 24, 2006) available at http://www.usdoj.gov/ag/speeches/2006/ag_speech_ 0601241.html [hereinafter Gonzales, Georgetown Remarks].

[34] As quoted in Unclaimed Territory, The Administration's New FISA Defense is Factually False, http://glenngreenwald.blogspot.com/2006/02/adminstrations-new-fisa-defense-is.html (Jan. 24, 2006, 16:11 EST)

[35] DNI Mike McConnell, Statement for the record, Hearing on Modernizing FISA Before the Senate Select Committee on Intelligence, May 1st, 2007

[36] McConnell statement before the House Committee on the Judiciary, Warrantless Surveillance and FISA, 110th Congress 21 (2007).

[37] Senate Select Comm. on **Intelligence**, Implementation of the Foreign **Intelligence Surveillance Act** of 1978, S. Rep. No. 97-691, at 9-10 (1982).

[38] Gerald F. Reimers II, Foreign Intelligence Surveillance Act, 4 J. Nat'l Security L. 55, 101 (2000)

[39]Kim Taiple, Whispering Wires and the Warrantless Wiretaps: Data Mining and **Foreign** Intelligence **Surveillance**, Bull. on L. & Sec. (Ctr. on Law & Sec., New York, N.Y.), Spring 2006, at 1, 5 and 6.

[40] Richard A. Posner, Op-Ed., A New **Surveillance Act**, Wall St. J., Feb. 15, 2006, at A16;

[41] William C. Banks, Programmatic Surveillance and FISA; Of Needles in Haystacks, 88 Tex.L. Rev. 1633 (2010) at 1653. The general context was an analysis of the FISA Court of Review Opinion In re Directives Pursuant to

Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004 (FISA Ct. Rev. 2008) pertaining to overseas surveillance of US persons, but the wording is directly on point.

[42] Mark Riebling, Uncuff the FBI, Wall St. J., June 4, 2002, at A20

[43] See U.S. v. Cavanaugh, 807 F.2d 787 (Ninth Cir. 1987) rejecting this argument based on the careful compliance of the government with the statute. See Frederick Frommer, Federal Judge: FISA Court Not a Rubber Stamp, AP NEWs, The Big Story, http:// app.org, and Richard Posner following.

[44] Richard Posner, Privacy, Surveillance and Law, 75 U.Chi.L.Rev. 245 (2008) at 260.

[45] David A. Vise & Vernon Loeb, Justice Study Faults FBI in Spy Case: Wen Ho Lee Probe Too Slow and Sloppy, Report Says, Wash. Post, May 19, 2000, at A1.

[46] See the Special Report of the DOJ Inspector General, A Review of the FBI's Handling of Intelligence Information Related to the September 11th Attacks, November 2004, Chapter Four, The FBI's Investigation of Zacarias Moussaoui, Introduction, http://www.justice.gov/oig/reports/2014/s1404.pdf

[47]Wall Street Journal, Surveillance and Shazad, supra note 17.

[48] Id.

[49] Keith Maart, The Boston Marathon Bombing One Year Later……A Detailed Look at the Vast Failures, Falsehoods and Cover-ups of the FBI and CIA, VT Military and Foreign Affairs Journal, http://www.veteranstoday.com/2014/04/13/the-boston-marathon-bombing-one-year-later-a-detailed-look/

[50] Fourth Amendment, U.S. Constitution

[51] Riley v. California 573 U.S. ____(2014) at 5 CITING Brigham City v. Stuart, 547 U.S. 398 (2006).

[52] Akhil Reed Amar, Fourth Amendment First Principles 107 Harvard Law Review 757 (1994) at 782-783.

[53] Colonnade Catering Corporation v. U.S. 397 U.S. 72 (1970).

[54] U.S. v. Biswell 406 U.S. 313 (1972).

[55] Camara v. Municipal Court of City and County of San Francisco, 387 U.S. 523, 534-539 (1967).

[56] Marshall v. Barlows, 98 S.Ct. 1816 (1978).

[57] In Re Sealed Case 310 F.3rd 717 (2002).

[58] Id.

[59] Id.

[60] In Re Directives Re Section 105 of FISA, FISA Court of Review, 551 F.3d 1004 (2008).

[61] Protect America Act of 2007, Pub. L. No. 110-55, §§ 2-3, 121 Stat. 552, 552-55 (codified at 50 U.S.C. §§1805(a)-(c)).

[62] FISA Amendments Act of 2008, Pub.L. No. 110–261, § 403, 122 Stat. 2436, 2473 (2008).

[63] Supra note 57

[64] In Re Directives at 1010

[65] Id. At 1012.

[66] Francesca Bignami, European versus American Liberty: A Comparative Privacy Analysis of Anti-terrorism Data Mining, 48 B.C.L. Rev. 609 (2007),Paul Schwartz, German and U.S. Telecommunications Privacy Law, 54 Hastings L.J. 751 (2003), Jeffery Brauch, Human Rights Protections in the Post 9/11 World, 31 Quinnipiac L. Rev. 339 (2013), Submission by EDRI and FREE to U.S. Congress and the European Parliament and the Council of Europe, August, 2013, http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/submission_us-europe_edri_final/submission_us-europe_edri_finalen.pdf

[67] Id. EDRI at p.13.

[68] Brauch supra note 178 and Mark Janis et al., European Human Rights Law 3 (2nd 3d. 2000)

[69] European responses to Snowden Revelations, http://irissproject.eu/wp-content/uploads/2013/12/IRISS_European-responses-to-the-Snowden-revelations_18-Dec-2013_Final.pdf at page 7 and see 13-14 for hypocrisy.

[70] Former NSA General Counsel Stewart Baker quoted in."Tom Gjelten, Which Citizens Are Under More Surveillance, US or European. http://www.npr.org/2013/07/28/206231873/who-spies-more-the-united-states-or-europe. Baker appears to be referring to a study by Hans-Jorg Albrech et al titled Legal Reality and Efficiency of the Surveillance of Communications under sections of the German Code, MPI 104 (2003). See Europe the Cloud and the New York Times. http://www.volokh.com/2013/10/16/europe-cloud-new-york-times/. Schwartz challenges the study on various grounds including the fact that the US does not count consensual monitoring and the MPI did.

[71] This will be noted in the section following. The ECtHR case holding that judicial approval is not necessary is Klass and Others v. Germany (1978) 2 EHRR 214. Numerous reformers are constantly advocating for judicial intervention but it is generally not required by law. A key survey was done by Christopher Wolf who summarized his findings with the following 2013 quote for NPR: "We can have a debate over whether or not the judicial and legislative approval process is working here in America, but the fact is, it exists, and in many places in Europe you don't have that kind of due process," Wolf says. "You don't have legislative oversight. In fact, the national security investigations are done completely in the dark or mostly in the dark. "Tom Gjelten, Which Citizens Are Under More Surveillance, US or European. http://www.npr.org/2013/07/28/206231873/who-spies-more-the-united-states-or-europe

[72] Lawfare, supra 181 at 2.

[73] http://www.echr.coe.int/Dociments/Convention_ENG.pdf

[74] Francesca Galli, "The Law on Terrorism: The UK, France and Italy Compared, Bruylant, at pages 92-93,

[75] 18 USC 2518 Section 3(c).

[76] ECtHR, Weber and Savaria v. Germany No. 54934/00 29 June 2006 paragraphs 93-94. See also Malone v. U.K. No. 8691/79, 26 April 1985, Liberty and others v. U.K. No. 58243/00, 1 July 2008.

[77] Id. Paragraph 95 See Report of the European Union Agency for Fundamental Rights, Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU, 2015 at 19, supra note 9.

[78] Basic Law (or Constitution) of the Federal Republic of Germany May 23rd, 1949, last amended July 29th, 2009 (Federal Law Gazette I. p. 2248).

79 Jan-Hendrik Dietrich, Of Toothless Windbags, Blind Guardians and Blunt Swords: The Ongoing Controversy About the Reform of Intelligence Services Oversight in Germany, http://dx.doi.org/10/1080/02684527.2015.1017246

[80] See Article 100 c section 1 of the German Code of Criminal Procedure and Article 163f section 4 of the Code of Criminal Procedure which are explained and referenced in Case of Uzun v. Germany, ECtHR, App. No. 35623/05, 2 September 2010, at pages 14-19 in the context of discussing GPS surveillance.

[81] Act Governing the Parliamentary Control of Intelligence Activities by the Federation, Revised July 29, 2009,(Federal Law Gazette I. p. 2346) and Act Restricting the Privacy of Correspondence, Posts and Telecommunications, section 9, Act of June 26th, 2001, last amended July 3rd 2009 (Federal Law Gazette I. p. 2499.)

[82] Dietrich supra note 79 at 6.

[83] Act Restricting the Privacy of Correspondence, Posts and Telecommunications, section 3 (1), Act of June 26th, 2001, last amended July 3rd 2009 (Federal Law Gazette I. p. 2499.)

[84] Id. Section 3 (2).

[85] Id. Section 3 (a). This presumably refers to completely private areas as well as activities such as legal representation and journalism. Conversations with Jan-Hendrik Dietrich October 2015.

[86] Id. Section 10 (2).

[87] Dietrich supra note 79 at 10.

[8888] Id. And Section 15 Act Restricting Privacy of Correspondence, supra note 81.

[89] Dietrich supra note 79 at 9.

[90] See Act Governing Parliamentary Control Supra note 80, sections 2-14.

[91] Dietrich supra note 79 at 13.

[92] Id.

[93] Klass v. Germany supra note 71.

[94] Act Restricting the Privacy, supra note 81, section 4 (4).

[95] See U.S. v. Verdugo-Urquidez supra note 3.

[96] Dietrich, Of Toothless Windbags, supra note 79.

[97] Authors conversations with Professor Jan-Hendrik Dietrich and Judge Doctor Markus Loffelman, Munich, October, 2015.

[98] Malone v. United Kingdom (1984), 7 EHHHR 245

[99] Regulatory of Investigatory Powers Act 2000 c.23

[100] Simon McKay, Covert Policing, Law and Practice, 2015, Oxford University Press, p. 5.

[101] Kennedy v. United Kingdom, App No 26839/05 (ECtHR 2010).

[102] See McKay, supra note 97, the UK "almost unique in the international community" for this prohibition at p. 108.

[103] RIPA, s. 5, see also McKay supra 97 at p.93. See also Library of Congress, supra note 11, U.K. p.2

[104]RIPA s. 3 (b), 5 (2) (a), 5 (3), Section 2.4 and 2.5 of the Code of Practice , McKay at p.93,94, see also Winston Maxwell and Christopher Wolf, A Global Reality: Government Access to Data in the Cloud, A Logan Lovell's White Paper, May 23, 2012 http://www.hldataprotection.com/2012/05/articles/international-eu-privacy/hogan-lovells-white-paper-on-governmental-access-to-data-in-the-cloud-debunks-faulty-assumption-that-us-access-is-unique/ and the following white paper by Maxwell and Wolf, A Sober Look at National Security Access to Data in the Cloud, May 22, 2013 http://www.hldataprotection.com/2013/05/articles/international-eu-privacy/white-paper-cloud-national-security and Privacy International https:''www.privacyinternational.org/reports//surveillance-policies.

[105] RIPA, s. 6, all parties who may apply are listed in page 2 of the Code of Practice, see McKay supra note 96 at p. 95.

[106] RIPA s. 8(2), 8(3) and Code of Practice para. 4.2.

[107] RIPA s. 15-18, McKay p.102 et seq.

[108] RIPA s 15 (4).

[109] McKay, supra 97 at 103.

[110] Francesca Galli, The Law on Terrorism, UK, France and Italy Compared, Bruylant 2015 p. 101.

[111] Id. At 101

[112] Id, FN 27, page 96

[113] Id at 96-103

[114] RIPA s. 18 (7), McKay, supra note 97 at p.110

[115] See McKay Id. At 109 citing section 11, 12 and 18 exceptions.

[116] See European Committee on Fundamental Rights, supra note page 38.

[117] See McKay supra note 97 reviewing sections 57-65 of RIPA.

[118] Id. RIPA sections 57 et. Seq. McKay Id. At pp 367-370.

[119] RIPA sections 59 et seq. McKay Id. At 371

[120] Id.

[121] RIPA sections 61, 62 McKay Id. At 372-374

[122] Id. At 373

[123] Id. At 375

[124] Id. At 385

[125] Sarah St. Vincent, Investigatory Powers Bill Would Expand Intrusive Surveillance and Violate Human Rights, https://cdt.org/blog/uks-draft-investigatory-powers-bill-would-expand-intrusive-surveillance-violate-human-rights/

[126] St. Vincent, Id, MP David Davis Says Judges Won't Get Power to Interrupt Surveillance Under May's Plan, http://www.theguardian.com/politics/blog/live/2015/nov/04/surveillance-internet-snoopers-charter-may-plans-politics-live?page=with:block-563a30efe4b08eefa4b96e08#block-563a30efe4b08eefa4b96e08

[127] Article L-241-1 Code de la Securite Interieure (CSI)

[128] Id-L-241-2.

[129] Galli, supra note 110, page 107.

[130] Kruslin v. France (1990) 12 EHRR 397

[131] *Loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques.*

[132] Lo1 n 2004 -204 du 9 mars 2004 portant adaption de la justice au evolutions de la criminalite

[133] *Loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers. Loi n° 2012-1432 du 21 décembre 2012 relative à la sécurité et à la lutte contre le terrorisme.*

[134] *Lambert v France*, App. no. 23618/94, (1998) ECHR 1998-V 86. See also *Matheron v France*, App no 57752/00, (ECtHR, 29 March 2005).

[135] Article 100 et seq Code de Procedure Penal

[136] Galli, supra note 110, p. 107, citing also J. Pradel, 'Un exemple de restauration de la légalité criminelle' *Dalloz* (1992): 49.

[137] Galli, supra note 110, page 109.

[138] Galli, Id. at p.110.

[139] See discussions of Germany, Italy, France and UK infra.

[140] 646/91 supra note 126 articles 3-19.

[141] Ordinance number 2012-351 12 March, 2012, see French Ministry of the Interior "The Legislative Part of the Code of Internal Security is Public" March 15th, 2012 http://www.interieur.gouv.fr/Archives/Archives-des-actualites/2012/Volet-legislatif-du-code-de-la-securite

[142] Article L 242 of the Code de la Securite Interieure (CSI)

[143] Article L 243-1 and R 244-1 et seq of the CSI

[144] See Report of the European Union Agency for Fundamental Rights, Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU, 2015, supra note 9 p. 46, citing CSI Articles L.831-1 to L. 833-11.

[145] See European Agency for Fundamental Rights, supra note 9 at 46, citing CSI Articles L. 801-1 -833-11.

[146] Library of Congress, Supra note 11, France, page 2.

[147] Galli, supra note 110, page 112.

[148] Article L 246 of the CSI

[149] Article 40 of the Code de Procedure Penal

[150] See European Union Agency for Fundamental Rights, Supra note, Sections 2.2 and 2.3, pages 34 et seq

[151] Id at p. 38, citing France, Ordinance No. 58-1100 on the functioning of the parliamentary assemblies, Art. 6 nonies, I 4°. See also France, Urvoas, J.-J., Parliamentary Delegation on Intelligence (2014), p. 13 and following and Urvoas, J.–J (2015), p. 41 and following.

[152]See Library of Congress, Foreign Intelligence Gathering Laws, 2014, supra note 11, https://www.loc.gov/law/help/foreign-intelligence-gathering/index.php, France, p.2.

[153] Galli, supra 110 at 113

[154] Id.

[155] Article 266 et seq Italian Codice de Procedura Penale (CPP)

[156] Article 266(1) CPP

[157] Article 267(1)

[158] Galli, supra note 110 at 115 and Celine Cocq and Francesca Galli, "The Catalysing Effect of Serious Crime on the Use of Surveillance Technologies for Prevention and Investigation Purposes, p. 268

[159] See *Legge 12 luglio 1991, n. 203 Conversione in legge, con modificazioni, del decreto-legge 13 maggio 1991, n. 152, recante provvedimenti urgenti in tema di lotta alla criminalità organizzata e di trasparenza e buon andamento dell'attività amministrativa.Ref as Law 203/1991.* Legge 11 agosto 2003, n. 228, Misure contro la tratta de persone Legge 15 dicembre 2001, n. 438 modificazoni legge 18 octobre 2001 n.374 recante disposizioni urgente per contrastareil terrorisimo internazionale.

[160] Article 277 CPP

[161] See G. Illuminati (ed), *Nuovi profili del segreto di stato e dell'attività di intelligence* (Torino: Giappichelli, 2011).

[162] Classified Information Procedures Act, 18 U.S.C. App III

[163] See Legge 15 dicembre 2001, n. 438 modificazoni legge 18 octobre 2001 n.374 recante disposizioni urgente per contrastareil terrorisimo internazionale.

[164] Id.

[165] Legge 31 luglio 2005, n.155 Conversionione in legge , con modificazioni, legge 27 luglio 2005, n.144, recante misure urgenti per contrast del terrorisimo internazionale.

[166] Legge, Sistema de Informazione per la sicurezza della Repubblica , Articles 6, 7 of law n.124, 2007

[167] See article 5(5) of 438/2001 supra note 159.

[168] See Italian court cases cited at Cass pen 29 October 1998, no 4977 (unrep); Cass pen 10 November 2000 no 11500 (unrep).

[169] http://www.garanteprivacy.it/home_en

[170] Legislative Act n.124 of 08/03/2007, reported on the Official Gazette of the Italian Republic, General Series, n.187 of 08/13/2007.

[171] Galli, supra note 110 at 121.

[172] Article 18.3 of the Spanish Constitution cited in Susana Sanchez Ferro, The Spanish Intelligence Service: New Threats, Same Secrecy, Better Oversight.http://heinonline.org/HOL/LandingPage?handle=hein.journals/vioincl4&div=35&id=&page=,at 432.

[173] Ley 11/2002, de 6 de mayo, del Central Nacional de Inteligencia

[174] Valenzuela Contrera v. Spain, 30 July 1998, Report 1998 V.

[175] Cited in Ferro at 437

[176] Provisions of Lawful Real Time Interception Assistance, Spain, Telecommunications Industry, https://www.telecomindustrydialogue.org/resources/spain/

[177] Susana Sanchez Ferro, The Spanish Intelligence Service: New Threats, Same Secrecy, Better Oversight. http://heinonline.org/HOL/LandingPage?handle=hein.journals/vioincl4&div=35&id=&page=,at 432.

[178] Ley 11/2002, de 6 de mayo, del Central Nacional de Inteligencia

[179] Id. Article 4.

[180] Ferro, supra 172 at 433.

[181] Article 4 (d) cited at Ferro 434.

[182] Report of the European Union on Fundamental Rights, supra note 9, at 39.

[183] Ferro, supra note 172 at 441

[184] Ley Organica 2/2002 del Control Judicial Previo de Centro Nacional de Inteligencia.

[185] Ferro at 437 citing Judicial Oversight Act

[186] Id.

[187] Id.

[188] Provisions of Real Time Lawful Interception Assistance, supra note 168.

[189] Id.

[190] See lengthy sections on proposed reforms in McKay supra 97 and Galli supra note 107. See report of the European Union on Fundamental Rights, supra note 9, at 56.

[191]See Report of the European Union id. At 66.

[192] CIA v. Sims, 471 U.S. 159 (1984)

[193] Id. At 176

[194] Id. At 178

[195] Report of the European Union, supra note 9 at 56.

[196] Klass and others v Federal Republic of Germany, European Court of Human Rights (Series A, NO 28) (179-80) 2 EHRR 214, 6 September 1978, at 26, paragraph 56,quoted in Saperstein, supra note 29 at 1977.

[197] See Nat'l Comm'n on Terrorist Attacks upon the U.S., The 9/11 Commission Report 416-19 (2004), p.79 et seq, Legal Constraints on the FBI and the Wall.

For excellent quotes from former high ranking DOJ officials on problems created by the wall, see Nola Breglio, Leaving FISA Behind; The Need to Return to Warrantless Intelligence Surveillance, 113 Yale L.J. 179 at 193-194. The "wall" and its effects are explained in detail in Ronald J. Sievert, Patriot 2005-2007; Truth, Controversy and Consequences, 11 Texas Review of Law and Politics 2, pp.322-331 (2007). The Patriot Act as upheld by In Re Sealed Case, US Foreign Intelligence Surveillance Court of Review, 310 F.3d 717 brought down the wall.

[198] New York City Police Commissioner Raymond Kelly cited in Wall Street Journal, Surveillance and Shazad, Are Wiretap Limits Making it Harder to Discover and Pre-empt Jihadists. http://online.wsj.com/news/articles/SB10001424052748704250104575238444182924 96.

[199] See examples cited pages 9-10 previous.

[200]See Ian Cameron, National Security and the European Convention on Human Rights 110, discussing the incompatibility between rigorous legal standards and national security objectives., quoted Daniel Saperstein, The European Counterterrorist as the Next Cold Warrior 32 Fordham Int'l L.J. 1947 (2009at 1975-1976.

[201] Jeffery Brauch, Human Rights Protections in the Post 9/11 World, 31 Quinnipiac L. Rev. 339 (2013), Submission by EDRI and FREE to U.S. Congress and the European Parliament and the Council of Europe, August, 2013, http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/submission_us-europe_edri_final/submission_us-europe_edri_finalen.pdf

Ronald J. Sievert

Professor Sievert graduated from St. Bonaventure University in 1970, served four years as an Army officer and graduated from the University of Texas School of Law in 1977. He joined the US Department of Justice in 1983. After trying several major violent crime, corruption and fraud cases he was named a DOJ Senior Litigation Counsel, Chief of the Criminal Division of the Eastern District of Texas, Chief of the Austin Division of the Western District of Texas and DOJ Assistant Director in Charge of the evaluation of all of the nation's US Attorney's offices.

In 1990, he was assigned to DOJ's National Security Working Group and as an International and National Security Coordinator for the Department as well as legal advisor to the Central Texas Counter Terrorism Working Group. As INSC he worked closely with the FBI and US intelligence agencies on both international and national security related cases, trained federal prosecutors, and has traveled to Kosovo, Qatar, Israel and England to teach foreign judges and prosecutors and investigate international and national security matters. He began teaching at the FBI Academy and US Department of Justice Advocacy Institute in 1985.

In 2000, he took a leave of absence to teach National Security Law and Federal Criminal Law at the University of Texas School of Law and has continued teaching as an adjunct professor at UT Law. He has received several awards for his work including the Department of Justice Directors Award for Superior Performance on two occasions and awards from several government agencies. He has published two books, Cases and Materials on US Law and National Security (2000, third edition 2012) and Defense, Liberty and the Constitution (2005) as well as eleven Law Review Articles on legal issues related to national security.

The Bush School of Government and Public Service

Mark Welsh, Dean and Holder of the Edward & Howard Kruse Endowed Chair

Founded in 1997, the Bush School of Government and Public Service has become one of the leading public and international affairs graduate schools in the nation. One of ten schools and colleges at Texas A&M University, a tier-one research university, the School offers master's level education for students aspiring to careers in public service.

The School is ranked in the top 12 percent of graduate public affairs schools in the nation, according to rankings published in U.S. News & World Report. The School now ranks thirty-third among both public and private public affairs graduate programs and twenty-first among public universities.

The School's philosophy is based on the belief of its founder, George H.W. Bush, that public service is a noble calling—a belief that continues to shape all aspects of the curriculum, research, and student experience. In addition to the Master of Public Service and Administration degree and the Master of International Affairs degree, the School has an expanding online and extended education program that includes Certificates in Advanced International Affairs, Homeland Security, and Nonprofit Management.

Located in College Station, Texas, the School's programs are housed in the Robert H. and Judy Ley Allen Building, which is part of the George Bush Presidential Library Center on the West Campus of Texas A&M. This location affords students access to the archival holdings of the George Bush Presidential Library and Museum, invitation to numerous events hosted by the George Bush Foundation at the Annenberg Presidential Conference Center, and inclusion in the many activities of the Texas A&M community.

The Scowcroft Institute of International Affairs

Andrew S. Natsios, Director and E. Richard Schendel Distinguished Professor of the Practice

The Scowcroft Institute of International Affairs (SIIA) is a research institute housed in the Bush School of Government and Public Service at Texas A&M University. The Institute is named in honor of Lt. Gen. Brent Scowcroft, USAF (Ret.), whose long and distinguished career in public service included serving as National Security Advisor for Presidents Gerald Ford and George H.W. Bush. The Institute's core mission is to foster and disseminate policy-oriented research on international affairs by supporting faculty and student research, hosting international speakers and major scholarly conferences, and providing grants to outside researchers to use the holdings of the Bush Library.

"We live in an era of tremendous global change. Policy makers will confront unfamiliar challenges, new opportunities, and difficult choices in the years ahead. I look forward to the Scowcroft Institute supporting policy-relevant research that will contribute to our understanding of these changes, illuminating their implications for our national interest, and fostering lively exchanges about how the United States can help shape a world that best serves our interests and reflects our values."

— Lt. Gen. Brent Scowcroft, USAF (Ret.)