Security versus Liberty: Striking the Right Balance. A Comparison of Anti-Terror Provisions in India and the United States

By Sheetal Asrani
Suggested Citation: Sheetal Asrani, *Security versus Liberty: Striking the Right Balance. A Comparison of Anti-Terror Provisions in India and the United States*, 3 German Law Journal (2002), *available at* http://www.germanlawjournal.com/index.php?pageID=11&artID=186
SPECIAL FORUM ISSUE: THE WORLD WE (INTERNATIONAL LAWYERS) ARE IN: LAW AND POLITICS ONE YEAR AFTER 9/11. I. Introduction: [1] *Ahmad Omar Saeed Sheikh. A Britishborn Muslim arrested by Indian authorities in connection with the kidnapping of four British and American backpackers in Kashmir in 1994. Released in exchange for the passengers and crew of Indian Airlines flight IC 814 hijacked to Kandahar, Afghanistan on December 25, 1999. Suspected of al-Qaida links and sentenced to death by a court in Pakistan for the kidnap and murder of U.S. journalist Daniel Pearl in January 2002. [2] India, U.S.A. and the U.K. – three countries caught up in a web of Islamic terrorist links and activities.* [3] In this paper I want to discuss the legislative responses to the terrorist threat in India and the United States in the aftermath of September 11 and the attack on India\'s Parliament three months later. (1) I will examine the civil liberty risks involved in the use of increased law enforcement and intelligence-gathering powers under new anti-terror laws, and their effect in particular on two areas – firstly, the right to privacy and secondly, the right to freedom of speech. (2) While my paper does not offer any solutions, it is an attempt to explore some problematic issues in the trade-off between national security and individual liberties. **II. Mapping the Political Process:** [4] Both India and the United States enacted anti-terrorism laws in the immediate aftermath of September 11. Although these laws arguably cut deeper into the system of personal liberties than any other piece of legislation in recent years, they were also rushed through the legislative process faster than any other law in recent years. The Indian government capitalized on the shift in U.S. policy after September 11 by responding immediately and decisively in offering its full support for the American \"War on Terrorism\". (3) Prompted ostensibly by India\'s own problems with terrorist violence, as well as to some degree, by Prime Minister Vajpayee\'s desire to portray himself as a leader in the campaign against terrorism (at least in South Asia), the government hastily pushed through Parliament the controversial Prevention of Terrorism Act, 2002 (POTA). (4) [5] Notwithstanding its numerous potentially objectionable provisions, the procedure by which it was enacted was a matter of concern in itself. Rather than being piloted through Parliament as a Bill, POTA was promulgated as an Ordinance four weeks before Parliament opened for its winter session. (5) The use of this fast-track procedure enabled the government to bypass the requirement of submitting the text to the Parliamentary Standing Committee on Home Affairs and the National Human Rights Commission for examination and comment. This move by the government was interpreted by political opponents as an attempt to bring in the new measures to combat terrorism through the ‘back door\', provoking strong criticism. [6] After the Bill was rejected in the Upper House in which the governing party (Bharatiya Janata Party or BJP) lacks a majority, a rare joint session of both Houses was called. The BJP coalition\'s majority in the combined 782-member Parliament allowed the Bill to go through. The only two joint sessions that have taken place in the past in India were preceded by a general consensus; however, the government refused to forge a consensus on POTA by referring it to a Select Committee of Parliament for deliberations as mandated for every Bill. [7] On a similar note, in the U.S., key procedures applicable to proposed laws - including inter-agency review and the normal Committee and hearing processes - were suspended for the enactment of the USA PATRIOT Act. (6) Just six weeks after September 11, the U.S. Congress yielded to the Bush administration\'s demands for a new arsenal of anti-terrorism weapons and overwhelmingly approved this new law. (7) The hastily-drafted, complex and far-reaching legislation spans 342 pages. Yet it was passed with virtually no Congressional or public debate. [8] In India however, fears about POTA have been evaluated against the Indian experience with the Terrorist and Disruptive Activities (Prevention) Act, 1987 (TADA), an anti-terror law under which more than 76,000 individuals were arrested for carrying out obscurely-defined \"anti-national\" and \"disruptive activities\". TADA was allowed to lapse in 1995 following a sustained campaign by the National Human Rights Commission, together with domestic and international human rights organizations. (8) TADA charges against almost 24,000 people were dropped on the recommendations of Review Committees constituted under a Supreme Court directive. (9) [9] The Indian government sought to justify the passage of POTA as being necessary to fill the vacuum created by the lapse of TADA, thereby giving law enforcement authorities more \"teeth\". It was argued that the current criminal justice system was not equipped to deal with ‘heightened threats\' post 9/11. Existing laws in India did not define a terrorist act, terrorist organization, proceeds of terrorism or the financing of terrorist organizations. Moreover, it was argued that unlike TADA, the Act incorporated a number of safeguards against the misuse of power by law enforcement agencies. **III. The Right Solution?** [10] One might legitimately question whether attacks similar to the one carried out on the Indian Parliament on December 13, 2001, might have been prevented by these enhanced powers. It would seem not, as the Prevention of Terrorism Ordinance (POTO) was already in force when the assault occurred. On the contrary, concerns that POTA might be used to target political opponents and minority groups have been reinforced: when Hindu-Muslim clashes erupted in Gujarat in March this year, 62 Muslims were charged under POTO. However, not one of the Hindu extremists responsible for the retaliatory anti-minority violence was similarly charged. Although the POTO charges against the accused were subsequently dropped, the suspicion that the new law is infected with religious discrimination is likely to have been

strengthened by such actions. [11] In the U.S., on the other hand, it appears that there was sufficient information for the U.S. intelligence and military to have taken steps to detect and prevent a September 11-like scheme. (10) The national security establishments under both Bill Clinton and George Bush, Jr. failed to heed information dating back to 1995 warning of the heightened possibility of airliner attacks. These leads were small pieces of data among the massive amounts of material swept up by the sprawling intelligence apparatus. (11) While the objective of the PATRIOT Act is the strengthening of the anti-terror campaign by the enhancement of the intelligence-gathering powers of government agencies, information that has now come to light would seem to suggest that the root of the problem might have lain more in the effectiveness of the response to intelligence already available to the CIA and the FBI prior to the attacks. The imperative now would rather seem to be a get-down-to-business accounting of the inertia or negligence that preceded September 11 – an inquiry that could begin the long-overdue reformation of CIA and FBI operating practices. (12) Instead of investigating the failures of policy, imagination and co-ordination over two administrations, the administration\'s response has been a call for greater secrecy in government, and a suggestion that anyone who dares question the need for amplified powers bestowed under PATRIOT is ‘unpatriotic\'. [12] While it remains to be seen how the executive will wield its new authority, if the months that have elapsed since September 11 are any guide, it would appear that we should brace ourselves for a disregard of the rule of law by the very agencies charged with its enforcement. By November 2001, the Department of Justice had already detained more than 1,100 immigrants, not one of whom has been charged with committing a terrorist act and only a handful of whom are being held as material witnesses to the 9/11 hijackings. (13) **IV. The Need for Patrol on the Information Superhighway: Right to Privacy and the Anti-Terror Legislation** [13] From deep within the mountains in Afghanistan, Osama bin Laden was able to plan, finance, recruit for and carry out the September 11 attacks. This was made possible by the internet, electronic mail, chat rooms, instant electronic messaging, electronic banking, mobile phones and satellite links. This suggests a need for a 21st century approach to electronic surveillance. The challenge however, is the crafting of a law that finds the middle ground in satisfying the desire for online privacy as well as national security from international terrorism. [14] Both the PATRIOT Act and POTA have enlarged the executive\'s powers in the field of conducting searches, electronic surveillance and intelligence-gathering, running squarely into privacy rights that enjoy constitutional protection. **1. PATRIOT Act and the Fourth Amendment:** [15] The Fourth Amendment to the U.S. Constitution \"protects the right of the people to be secure in their persons, houses, papers and effects against unreasonable searches and seizures\". This right \"shall not be violated but upon probable cause\". In the following paragraphs, I will examine how three sections of the PATRIOT Act relating to ‘sneak and peak\' searches (Section 213), wiretaps (Section 218) and internet surveillance (Section 216) collide with this constitutional guarantee. *a) Sneak and Peak* [16] Consider this: U.S. law enforcement officials may now covertly enter and search your home or office without notifying you of the execution of the search warrant until after the search has been completed. Section 213 of the PATRIOT Act legitimizes \"sneak and peek\" searches where \"providing immediate notification may have an adverse result.\" [17] While notice of the search may be delayed for \"a reasonable period,\" the Act does not spell out what length of time may be deemed reasonable. Moreover, Section 213 is not limited to terrorist investigations, but extends to every manner of criminal investigation. Alarmingly, Congress has not scheduled this Section to expire. *b) Wiretaps* [18] A seemingly minor alteration in language relating to wiretap authorizations has succeeded in blurring the distinction between intelligence investigations and criminal investigations. (14) A federal officer can now monitor a private phone conversation without a warrant merely by claiming that the gathering of foreign intelligence constitutes a \"significant purpose\" of the investigation. Prior to the PATRIOT Act, the standard for the authorization of surveillance was more stringent, and required the showing that foreign intelligence-gathering was the \"primary purpose\" of the surveillance. [19] The concern with Section 218 is that agents will now deliberately circumvent the Fourth Amendment by bringing applications for wiretaps under the guise of an intelligence investigation, when the real purpose of the surveillance is a criminal investigation, with no showing of probable cause that a crime has been or will be committed. (15) This is a provision that flies in the face of more than twenty years of sound case law. (16) [20] To give an example of how this might play out: an American of Sudanese ancestry, who resorted to an act of violence in protesting against the New Partnership for Africa\'s Development (NEPAD) at the G-8 Summit in Kananaskis might find himself the subject of surveillance under Section 218\'s lax standard. Here, the agent would claim as a ‘significant foreign intelligence purpose\' investigating the individual\'s potential al-Qaida links in Sudan, while the clear ‘primary purpose\' would be a purely domestic criminal investigation of the individual\'s activities, in derogation of the Fourth Amendment\'s probable cause guarantee. [21] Furthermore, since the PATRIOT Act does not define what constitutes a \"significant purpose\", it is uncertain how far the interpretation of this phrase will be stretched to accommodate law enforcement and intelligence agencies. However, considering that only one surveillance application has been refused in the last 22 years, (17) it is perhaps not too difficult to predict how this lenient standard will be implemented. [22] Section 218 also portends a significant minimization of judicial oversight of criminal investigations. As a result of this provision, initial surveillance of a target may continue for at least up to three months (three times longer than under normal criminal laws) before there is need for judicial review by a neutral judge. However, if at the end of ninety days agents decide not to apply for an extension of surveillance, their actions will never be reviewed. Since there is no provision for notice of completed surveillance to be given to targets, a person may never know that his conversations have been intercepted and his privacy invaded. [23] The use of Section 218 for surveillance in criminal investigations becomes even more attractive considering there is no requirement that the wiretapping agent ensure that his target is actually using a specific

telephone line. This would allow an agent to tap a phone for a potentially lengthy period of time in the hope of intercepting incriminating information from another source (non-target) using that line. This wiretapping power could thus be used for the indiscriminate surveillance of third-parties. Presuming no charges are brought against such non-target, the individual would not even learn of the surveillance. [24] Civil liberties groups have been up in arms that allowing agents to overcome the Fourth Amendment in criminal investigations will lead to a pervasive abuse of executive power along the lines of that which occurred in the sixties and seventies when thousands of Americans (including student activists and black nationalists) were illegally spied on by the CIA and FBI. (17) While the Senate fully recognized Section 218\'s potential for permitting the circumvention of the probable cause requirement, thereby infringing privacy interests, it decided to leave it to the courts to determine how far law enforcement agencies may use this power for criminal investigation and prosecution beyond the scope of the statutory definition of foreign intelligence information. (19) *c) Internet Privacy* [25] Under Section 216 of the Act, courts are required to order the installation of a pen register and a trap and trace device (20) to track both telephone and internet \"dialing, routing, addressing and signaling information\" anywhere within the U.S., when a government attorney has certified that the information to be obtained is \"relevant to an ongoing criminal investigation\", provided however that such information shall not include the ‘content\' of any communication. [26] Thus, to get an order for interception of internet activity, law enforcement must simply certify that the information is \"relevant to an ongoing criminal investigation.\" This suggests a very low threshold of proof, far less than ‘probable cause\', and PATRIOT extends this low standard beyond the mere \"trapping and tracing\" of telephone numbers, to tracing email and internet activity which is far more revealing than numbers dialed on a telephone. (21) As a result, the websites a person visits and terms entered into search engines – actual ‘content\' information – may now be monitored employing this low evidentiary standard. This is like giving law enforcement the power, based only on its own certification, to require a librarian to report on all the books a person peruses while visiting a public library. [27] Section 216 also authorizes the installation of an internet surveillance program dubbed ‘Carnivore.\' (22) Secretly launched in June 1999 but officially announced only a year later, Carnivore made cyber-snooping in America a reality much before the introduction of the PATRIOT Act. (23) While law enforcement officials gained access to specific accounts of Internet Service Providers (ISPs) even before Carnivore, the difference was the presence of a specific warrant for each suspect. (24) Carnivore consists of a small box with the formidable ability to intercept all forms of internet activity, including email messages, web page activity and internet telephone communications of all the customers of compliant ISPs. Carnivore\'s task is to filter the ISP\'s network traffic and identify and convert from binary code to human-readable form, information relating to the target only. (25) However, as Carnivore examines all network traffic to look for its target, there are two potential dangers: one, that it captures communications relating to non-targets, and two, that it does not filter out just transmission information, but captures the entire email content. (26) [28] Neither the accuracy of Carnivore\'s filtering system, nor the infallibility of its human programmers has been demonstrated. The only version of Carnivore that was publicly reviewed allowed the wholesale alteration of collected data without leaving any evidence of such alteration. (27) What this means is, it is impossible to definitively determine which agent set or changed the filter configuration, or what configuration was used to collect any given set of data. Moreover, the relationship between the configuration, the collected data and other investigative activities may be difficult to establish, and the time and date stamps placed on data collected are subject to error. (28) In light of this revelation, and without any public review of subsequent Carnivore versions, one may well question just how much control courts will have over the use of this powerful software. [29] Section 216 is not scheduled to expire. The government\'s already-broad monitoring capabilities are certain to evolve so that surveillance will become faster, cheaper, more covert and more intrusive. Until it is proven that technical limitations in the Carnivore program have been overcome, the judicial scrutiny provided for under the Act is merely illusory. *d) Comments* [30] While it is true that a citizen\'s expectation of privacy must in certain cases yield to the greater national security concerns of the government, what is particularly troubling about PATRIOT is that although it consolidates vast and permanent powers in the executive branch, at the same time, it insulates the exercise of these powers from meaningful judicial and Congressional oversight. Americans are being asked to adapt to the idea that law enforcement and intelligence agents may now sneak into their homes and offices, conduct a search of their personal effects, tap their phone lines and monitor their email, without their learning of the fact. All this in the name of ‘national security.\' [31] Will PATRIOT help pre-empt the next attack? Could PATRIOT have prevented September 11? [32] The case of Zacarias Moussaoui underscores that America\'s Achilles heel was not the lack of intelligence, but the lack of an effective identification of and response to already-available data. Moussaoui was arrested on August 16, 2001 following a tip-off from flight-school officials to the FBI about his suspicious conduct. Instructors claim that it allegedly took four to six phone calls to get the FBI to act. Moreover, despite the fact that FBI headquarters was notified by French intelligence that Moussaoui had al-Qaida links and Islamic extremist beliefs, he was not investigated. (28) FBI Director Bob Mueller has denied they had any information on Moussaoui that could have helped to predict or prevent the attacks. However, classified documents reveal that the FBI failed to act on clear clues because the investigation was \"sabotaged\" by infighting and careerism. (30) In another leak, it has also been revealed that President Bush received a memo on August 6 assessing the menace of al-Qaida and stressing that bin Laden was poised to hijack aircraft and attack targets in the U.S. (31) [33] While it is likely that some measure of individual liberties will have to be bartered for a greater sense of security, citizens should not have to face an unjustified, unchecked and permanent clampdown on their freedoms in order to pay for the administration\'s failure to heed intelligence warnings, even from foreign sources. The need of the hour would perhaps appear to be rather a re-

ordering of the priorities within the FBI, re-organization and structural reform, and an up-grading of technology. (32) Finally, it will be up to the courts to secure individual freedoms since the legislators were apparently not up for the job. **2. POTA and the Right to Privacy:** [34] In India, the backdrop is different in that there are as yet no laws protecting online privacy. Indian courts have not yet had an opportunity to address privacy issues such as control of private electronic data, cyber intrusions and electronic surveillance. While the Indian Constitution does not patently grant a \"right to privacy\", the Supreme Court has dealt with the issue by importing the right to privacy into the fundamental right to life and liberty under Article 21, (33) and the right to freedom of speech and expression in Article 19(1)(a). (34) *Ad hoc* judicial solutions have thus far been found sufficient to deal with individual cases as they have arisen. (35) However, the increased electronic interference portended by POTA will necessarily spur the carving out of a national legislation dealing with privacy rights. *a) Interceptions* [35] Section 38 of POTA provides that an application for an order allowing the interception of wire, oral or electronic communications may be made before an executive authority designated by the government. The application must disclose \"probable cause\" for the belief that such interception may provide \"evidence of any offence involving a terrorist act\". The investigating officer must specify the period for which such interception is to be authorized, which may not in any event exceed sixty days. [36] Every order passed by the Competent Authority is subject to review by a Committee set up under the Act for this purpose. If the Review Committee disapproves the order, Section 46(4) stipulates that the interception commenced shall be discontinued, and any intercepted communication already gathered shall be inadmissible as evidence. [37] While the Act does not make it mandatory for the intercepting officer to provide reports to the issuing authority showing progress made towards the objective and the need for continued interception, any application for extension of an order under Section 38(2)(e) must be supported by a statement setting forth the results thus far obtained, or an explanation of the failure to obtain such results. *b) Comments* [38] While it cannot be denied that law enforcement agencies require tools that put them on a level playing field with terrorists, PATRIOT at least would appear in many ways to stack the deck in favor of the government. It is possible that the Internet Age will evolve in such a way that what society is prepared to recognize as ‘reasonable\' may change. But until then, the PATRIOT Act would not appear to stand up against Fourth Amendment jurisprudence. POTA at a minimum lays the ground for judicial review of every interception order, and establishes a probable cause standard for authorizing interceptions. Moreover, POTA\'s context is limited to terrorism investigations, and does not encompass regular criminal investigations, as does PATRIOT. Again, while some of PATRIOT\'s most controversial provisions are not scheduled to sunset, POTA will have a life of only three years. The Indian Act does, however, suffer from a lack of clarity in that it does not make any distinction between ‘content\' and ‘tracking information\', or specify exactly what sort of private electronic data is liable to interception. It therefore falls to the Indian courts to interpret the Act progressively so as to safeguard fundamental rights against executive excesses. **3. Gagging the Marketplace? Right to Freedom of Speech and Association and the Anti-Terror Legislation** [39] The second area in which a collision between the new anti-terror laws and civil liberties may be anticipated is that of the right to freedom of speech and association. Both the Indian and American Constitutions articulate the right to disagree with the policies of the government, support unpopular political causes, and associate with others in the peaceful expression of those views. Unjustified investigations and criminalization of political expression are counterproductive and ultimately have a debilitating effect on the political system. Is freedom of speech such a barrier to the effective tackling and prosecution of terrorists? Does national security require restrictions calculated to stifle political dissent? These are perhaps important questions to bear in mind when evaluating the following new anti-terror provisions. **4. PATRIOT Act and the First Amendment** [40] The First Amendment to the U.S. Constitution makes inviolable both freedom of speech and freedom of association: \"The State shall make no law abridging the freedom of speech, or of the press, or the right to assemble peacefully.\" Promoting the truth, it has been famously argued, is best achieved by testing opinions in a free marketplace of ideas. (36) Holmes\' envisioned marketplace of ideas is potentially threatened by PATRIOT\'s over-broad definitions of ‘domestic terrorism\', ‘terrorist organization\', and ‘engage in terrorist activity\'. [41] Section 802 of the PATRIOT Act creates a federal crime of *\"domestic terrorism\"* under which anyone who tries to \"influence the policy of the government by intimidation or coercion,\" if his actions \"break any criminal laws\" and \"are dangerous to human life,\" is a terrorist. A1960\'s anti-Vietnam War protester would arguably have fit this new definition. [42] Because this crime is couched in such expansive terms, it may well be read by federal law enforcement agencies as licensing the investigation and surveillance of political activists and organizations based on their opposition to government policies, and lead to the criminalization of legitimate political dissent. (37) Vigorous political activities, by their very nature, could be construed as acts that \"appear to be intended to influence the policy of the government by intimidation or coercion.\" Further, acts of civil disobedience - even those that do not result in injury and are entirely non-violent – could be construed as \"dangerous to human life\" and \"in violation of criminal laws.\" In other words, if a protester at a peaceful demonstration against the launch of missile strikes against Iraq tore down a fence, and someone fell and injured his head, the sponsoring organization would now be liable to become the target of a federal investigation for terrorism. [43] Past records of wholesale abuses of law enforcement authority to harass individuals and organizations with unorthodox or unpopular political views are well-documented. (38) What makes Section 802 especially disturbing is that individual acts of violence at public demonstrations are already penalized under various criminal laws. It is difficult to understand the reasoning behind equating such actions with the acts of terror that took place on September 11. Moreover, there are already three definitions of terrorism in usage – international terrorism, terrorism transcending national borders and federal terrorism – which together sufficiently characterize the various manifestations of terrorism. (39) Therefore it remains

unclear why a fourth, broad definition as embodied in Section 802 is necessary. [44] Again, the Act empowers the Attorney General to authorize electronic surveillance without a court order and without judicial review. The manner in which the government implements the Act will therefore require monitoring so as to ascertain whether activists and organizations are being targeted selectively for surveillance and prosecution based on their opposition to government policies. [45] To complicate and obscure matters further, the term *\"terrorist organization\"* is no longer limited to organizations that have been officially designated as terrorist and that have therefore had their designations published in the Federal Register. Instead, Section 411 now includes as \"terrorist organizations\" groups that have never been designated as terrorist, if they fall under the loose criterion of \"two or more individuals, whether organized or not,\" which engage in specified terrorist activities. [46] After PATRIOT was enacted, Secretary of State Colin Powell created a list of organizations and individuals considered to be terrorists with virtually no Congressional or judicial oversight. . Under the Act, the Secretary of State has the sole authority to add individuals or organizations to the list of suspected terrorists. (40) [47] Certain provisions of the PATRIOT Act also have significant consequences for the status of immigrants and their continued residence in the U.S. Since 1983, the U.S. government had defined the term *\"terrorism\"* as \"premeditated, politically motivated violence perpetrated against non-combatant targets by sub-national groups or clandestine agents, usually intended to influence an audience\". (40) However, Section 411 of PATRIOT, which deals with immigrants, stretches the term to encompass any crime that involves the use of a \"weapon or dangerous device\" (other than for mere personal monetary gain). This section has potentially huge ramifications in that it vastly widens the class of non-U.S. citizens that can now be deported from the U.S. on terrorism grounds. (42) [48] The term *\"engage in terrorist activity\"* has also been expanded to include soliciting funds for, soliciting membership for, and providing material support to, a \"terrorist organization\", even when that organization has legitimate political and humanitarian ends and the non-citizen seeks only to support these lawful ends. In such situations, Section 411 would permit guilt to be imposed solely on the basis of political associations protected by the First Amendment. [49] By virtue of these provisions, non-citizens could be detained or deported for providing assistance to groups that are not designated as terrorist organizations at all, as long as the activity of the group satisfies an extraordinarily broad definition of terrorism that covers virtually any violent activity. (43) So now, environmental groups demonstrating against the drilling in the Arctic National Wildlife Refuge or human rights groups protesting the threatened withdrawal of American soldiers from U.N. peacekeeping operations would, on the basis of minor acts of violence or vandalism, meet this overbroad definition. Non-citizens who provide assistance to such groups - such as paying membership dues - will run the risk of detention and deportation. [50] What is disturbing is that most of these powers do little to increase the ability of law enforcement or intelligence to bring terrorists to justice, but much to undermine the Constitution and violate the rights of both immigrants and American citizens alike. Tackling these issues has become difficult at a time when public opinion is so thoroughly imbued with an unquestioning patriotic spirit. **5. POTA and the Right to Free Speech:** [51] Shifting the focus back to India, freedom of speech and expression is protected by Article 19(1)(a) of the Constitution. Clause (1)(c) of Article 19 articulates the right to form associations or unions. I will now discuss how the new definitions for ‘terrorist act\' and ‘terrorist organization\' impinge upon these constitutionally guaranteed rights. [52] Section 3(1) of POTA defines a *\"terrorist act\"* as \"any act done by any means whatsoever, with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in any section of the people, in such manner as likely to cause death or injury, or loss or damage of property, or *disruption of any supplies or services essential to the life of the community*.\" This wide definition has raised concerns that non-violent human rights defenders, minority communities and the media may be exposed to a discriminatory enforcement of the Act. While one of POTA\'s much-touted improvements over TADA is that it does not cover \"disruptive activities\" which were so ill-defined under the earlier Act as to allow the prolonged detention of striking students or milkmen, the phraseology of the definition of \"terrorist act\" in POTA arguably leaves the door open to equal abuse. [53] The Schedule to the Act designates a list of proscribed *\"terrorist organizations\"*. (44) This list may be added to by the government if an organization is \"believed to be involved in terrorism\". Section 18(4) is intentionally vague in its terms: an organization is deemed to be \"involved\" in terrorism if - (a) it commits or participates in acts of terrorism, or (b) prepares for terrorism, or (c) promotes or encourages terrorism, or (d) *is otherwise involved in terrorism.* [54] It is difficult to fathom the justification for a power to ban terrorist organizations which is *prima facie* so broad and open-ended as to be easily liable to abuse. Unlike the PATRIOT Act however, POTA has put in place a system of checks and balances. Section 19 of POTA provides for the review of orders banning terrorist organizations by a Committee headed by a Judge of the High Court. [55] Another striking provision states that a person commits an offence under Section 21(2) if he manages or arranges a meeting which he knows is - (a) to support a terrorist organization, or (b) to further the activities of a terrorist organization, or (c) to be *addressed by a person who belongs or professes to belong to a terrorist organization.* [56] Translated into practice, this could mean that the holding of any meeting of three or more persons, one of whom chances to belong to a terrorist organization is *ipso facto* criminalized, notwithstanding that the content of such a person\'s address did not relate to the inviting of support for, or the furthering of the activities of, the terrorist organization of which he is a member. [57] POTA\'s criminalization of acts \"threatening the unity, integrity, security and sovereignty of India\" (45) appears to be as broad as the PATRIOT Act\'s punishment of acts \"appearing to be intended to influence the policy of the government by intimidation or coercion\". (46) In the case of both sections, the danger to human life need only be a remote possibility. In the Indian Act, there is moreover the added danger that legitimate peaceful protest against the government which causes a disruption of essential services or supplies is branded a ‘terrorist act\'. [58] Although the

government\'s power to ban ‘terrorist organizations\' under POTA is broad, the Act does ensure the review of such orders. In contrast, the absence of any oversight mechanisms in PATRIOT with respect to the Secretary of State\'s power to proscribe ‘terrorist organizations\' is especially troubling. Whether the exigencies of combating terrorism warrant and vindicate these provisions will have to be borne out when their constitutionality is challenged. **V. Lessons from the United Kingdom:** [59] Sheikh Omar, (47) Zacarias Moussaoui (48) and Richard Reid (49) all lived and/or studied in England. Radical Islamic organizations, shadowy European revolutionary cells, and an assortment of liberation armies from the developing world have for a long time been basing themselves in Britain. In response to pressure from a number of foreign governments, the U.K. Government introduced a new law directed at international militant groups even before the terror attacks of September last year. (50) [60] While space constraints do not permit a detailed discussion of British anti-terror laws here, it is interesting to note how the U.K., which has waged a prolonged and deadly struggle against both domestic and international terrorism for decades, has chosen to deal with the problem. Not all of Britain\'s lessons are positive: many of its traditional civil liberties have been compromised. (51) Yet it is arguable that the odds of being blown up by a bomb in a bar during one of the IRA\'s periodic mainland bombing campaigns were not significantly less before the most recent cease-fire, with all the measures introduced to combat the terrorist threat, than they were 30 years earlier. Moreover, the revelations of spectacular miscarriages of justice involving alleged IRA terrorists have surfaced over the last 15 years, exposing the British criminal justice system to justifiable criticism. (52) [61] After almost every upward ratchet in the level of terrorist violence, the government\'s response was to seek greater powers to render the nation safer. More often than not, Parliament obliged. And through it all, British governments of varying political tendencies enjoyed overwhelming public support in pressing for stronger laws. (53) [62] Governments in India and the U.S. are willing to adopt sweeping instruments to present at least the appearance of responding strongly and effectively to a widely-perceived threat. But as with many government initiatives, once a policy or program is in place, it becomes progressively harder to control or limit. The hard lesson to be learned from the British experience is that the initial curtailment of civil liberties in the U.K. turned out to be the starting point of a dynamic and continuing adjustment in the way the law is viewed and implemented as a tool in the struggle against terrorism. [63] National security types often assure us that wartime diminutions of civil liberties are only temporary. But the war on terrorism is likely to be a permanent war. Defense Secretary Donald Rumsfeld has said that the war will not be over until there are no terrorist organizations of potentially global reach left in the world. (54) The Administration\'s defenders might concede that civil liberties have been curtailed, but contend that if we have prevented another terrorist attack, it is worth the cost. The problem of course is that one cannot know what might have happened had the government respected basic principles like due process, political freedom and the rule of law. [64] Unless we understand that respect for basic human rights is as integral to our security as fighting terrorism, we are in danger of losing sight of what we are fighting for. (55) **VI. Concluding Remarks:** [65] It is not possible to effectively fight terrorism without addressing its roots. We have to recognize that ‘terrorists\' are, as Nicholas Kittrie points out in his book, ‘rebels *with* a cause\'. (56) And the cause of their animosity against the U.S. has much to do with American foreign policy, and the support for tyrannical and repressive regimes. This animosity has only proliferated and heightened with President Bush\'s \"War on Terrorism\", a campaign which makes no distinction between accepting the support of an extremist theocracy like Iran or a repressive autocracy such as Saudi Arabia. [66] Further, in prosecuting those who engage in politically-motivated violence, it is important to act in accordance with international law. America\'s response to the September 11 attacks (for instance, the indefinite detention of non-citizens under PATRIOT and the executive order permitting trials before military tribunals) is encouraging other countries to pursue repressive policies that will fuel terrorism rather than quench it. The anti-terror rhetoric has provided a new justification for the violation of human rights of nationals in Chechnya, China, and Israel, for example. [67] With terrorism being the sophisticated transnational enterprise it is today, POTA marks a step in the right direction in terms of allowing as admissible evidence intercepts of wire, oral and electronic communications. This will equip law enforcement officers with much-needed tools to pre-empt terrorist activities. However, a foreseeable problem in the processing of the huge volumes of data that the implementation of inflated surveillance laws will generate is the cost involved in terms of efficiency and investigative resources, particularly in the context of a country like India. Moreover, the patently discriminatory employment of the Act after the spate of violence in Gujarat only served to alienate more members of religious and ethnic minorities and radicalize groups that are already on the brink of using violence to pursue their ends. In the final analysis, such discrimination against citizen-groups of which terrorists represent a radical fringe will only backfire, resulting in additional recruitment to the terrorist cause, increased violence, and a reduction in the reserve of loyalty and patriotism within such groups. (57) The government\'s biggest challenge in the days ahead will be the impartial and judicious use of its powers under the Act. Ultimately in India, there will have to be a reckoning – socially, economically and politically – in order to address the causes breeding resentment that spur terrorist violence in many of the north-eastern states and Kashmir. [68] Our goal must be to evolve for the long-term an effective anti-terror strategy that tackles the underlying causes of grievance that allow terrorist networks to thrive. In the struggle ahead, we would accomplish far greater by embracing rather than undermining the rule of law.

∗ LL.M. (Harvard), Associate: Fried, Frank, Harris, Shriver & Jacobson, New York. I am grateful to Devashish

Bharuka, technology virtuoso and friend, for his prompt, invaluable inputs and endless patience. To Philipp Dann, for the roadmap, editorial comments, and encouragement throughout the writing of this piece, thank you. Producing this paper would not have been possible without your support.

(1) On December 13, 2001, five militants, allegedly belonging to the Lashkar-e-Taiba terrorist group and armed with explosives, mounted an unprecedented suicide attack on India\'s Parliament in New Delhi. For more information *see* New York Times Editorial, *An Assault on India\'s Democracy*, December 15, 2001.

(2) A discussion of the newly introduced - and quite controversial - provisions in the Indian Act relating to arrest, detention, bail, etc. is beyond the ambit of this paper.

(3) India was driven by the desire to further its rapprochement with Washington and sought a closer engagement with the United States after the twin tower attacks. For an interesting comment see Dennis Kux, *India\'s Fine Balance*, Foreign Affairs, May/June 2002.

(4) Act No. 15 of 2002, passed by Parliament on March 26, 2002. Presidential assent was received on April 2, 2002. For the text of the Act *see* http://216.239.51.100/search?q=cache:DHE9H9tc67kC:alfa.nic.in/rs/bills-ls-rs/5-c-2002.pdf+%22Prevention+of+Terrorism+Act+2002%22&hl=en&ie=UTF-8

(5) Article 123 of the Indian Constitution empowers the President to promulgate Ordinances when Parliament is in recess. However, such Ordinance would expire if not approved by Parliament within six weeks of its re-assembly. Parliament convened for its winter session on November 19, but POTO lapsed on December 31 and had to be re-promulgated. It was finally passed by Parliament only on March 26, 2002.

(6) Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (October 26, 2001). For the text of the Act *see* http://www.ins.usdoj.gov/graphics/lawsregs/patriot.pdf

(7) The House vote was 357-to-66, and the Senate vote was 98-to-1. The very title of the Act would seem to suggest that it would have been unpatriotic to vote against it, something that only one Senator had the courage to do.

(8) The implementation of the Act resulted in prolonged detention without charge or bail or trial, political torture, forced confessions, etc. The law was extensively used against college students, trade unionists, women\'s organizations, anyone \"inconvenient\". Parliament was to review the Act every two years.

(9) The rate of conviction under TADA was an appalling 0.9%.

(10) *See* David Corn, *The Warning Game*, The Nation, June 10, 2002.

(11) The U.S. government spends more than US$30 billion annually on spies and high-tech eavesdropping.

(12) Anonymous, *September 11 questions*, The Nation, June 10, 2002.

(13) The PATRIOT Act has expanded the Attorney General\'s already broad authority to detain non-citizens as suspected ‘terrorists\' with minimal procedural safeguards. Prolonged arbitrary detention of non-citizens is a violation of internationally recognized standards, and could encourage many authoritarian regimes around the world to do the same.

(14) Criminal investigations demand a much higher legal standard of demonstrated probable cause under the Fourth Amendment. When the government in conducting surveillance is primarily attempting to form the basis for a criminal prosecution, individual privacy interests come to the fore and government foreign policy concerns recede.

(15) In an opinion made public on August 23, 2002, it has been revealed that the secret Foreign Intelligence Surveillance Court has identified more than 75 cases in which it was misled by the FBI in documents in which the bureau attempted to justify its need for wiretaps and other electronic surveillance. In a stinging criticism, the court said the FBI and the Justice Department had, in a number of cases, made \"erroneous statements\" in eavesdropping applications about \"the separation of the overlapping intelligence and criminal investigators and the unauthorized sharing of intelligence information with FBI criminal investigators and assistant U.S. attorneys.\" This evidence of abuse of wiretap powers relates to cases as early as September 2000, even before PATRIOT\'s Section 218 lowered the standard for wiretap authorizations. For the full story, *see* Philip Shenon, *Secret Court Says FBI Aides Misled Judges in 75 Cases*, New York Times, August 23, 2002.

(16) *See* Sharon H. Rackow\'s Comment, *How the USA PATRIOT Act will Permit Governmental Infringement Upon the Privacy of Americans in the Name of \"Intelligence\" Investigations*, 150 U. Pa. L. Rev. 1651 (2002).

(17) Marcia Coyle, *Sharp Debate on Surveillance Law: Pick Between Two Little Words Makes a Big Difference*, Nat\'l L.J., Oct. 8, 2001, at A13.

(18) The absence of clear statutory or judicial standards led to widespread warrantless electronic surveillance of individuals who were not associated in any way with a foreign power, did not pose a threat to national security, and were not suspected of being involved in criminal activity. For more see Americo R. Cinquegrana, *The Walls (and Wires) Have Ears: The Background and First Ten Years of the Foreign Intelligence Surveillance Act of 1978*, 137 U. Pa. L. Rev. 793 (1989).

(19) 147 Cong. Rec. S10, 558 (daily ed. Oct 12, 2001) (statement of Senator Leahy).

(20) Pen registers record telephone numbers of outgoing calls. Trap and trace devices record telephone numbers from which incoming calls originate.

(21) Unlike telephone communications where the provision of dialing information does not run the risk of revealing content, email messages move together in packets that include both address and content information, making their separation difficult.

(22) The program is called DCS1000 or Carnivore because \"it chews all the data on the network\".

(23) Prior to the PATRIOT Act, the FBI claimed authority for the deployment of Carnivore in the internet context under statutory provisions originally enacted to regulate telephone surveillance. While courts issuing Carnivore pen register orders assumed these provisions extended to the internet, statutory authorization for pen registers to be utilized with non-telephone technologies was highly questionable. Section 216 by redefining pen registers to encompass internet applications brings the existing statutory language into line with actual practice, in which Carnivore has been employed by the FBI as an internet pen register on numerous occasions. *See* Anthony E. Orr\'s Note, *Marking Carnivore\'s Territory: Rethinking Pen Registers on the Internet*, 8 Mich. Telecomm. Tech. L. Rev. 219.

(24) To use an analogy, Carnivore allows the FBI to access an entire block of apartments on suspicion of just one tenant. They may not however search the other apartments or use the results of such illegal search. In support of the program, the FBI argued that smaller ISPs unlike AOL or excite.com cannot afford the capability to supply specific information, and for them, Carnivore is a necessary device. *See* http://www.svbizink.com/headlines/article.asp?aid=755&iid=155

(25) Section 216(3) of the PATRIOT Act requires that the record of such interception be provided under seal to the authorizing court within 30 days of the expiration of the order.

(26) It has been held by the United States Court of Appeals for the Armed Forces in *United States v. Maxwell*, 45 M.J. 406 (C.A.A.F. 1996) that an individual does have a reasonable expectation of privacy in his email transmissions. Interestingly enough, the United States Supreme Court has not yet had an opportunity to decide the issue.

(27) Illinois Institute of Technology Research Institute (IITRI), *Independent Technical Review of the Carnivore System: Draft Report*, November 17, 2000, at 4-4 to 4-5, available at http://www.usdoj.gov/jmd/publications/carnivoredraft1.pdf The Report states: \"Since there are no checksums or other protections on the collected data files and no individual accountability, anyone could edit the collected data and evidence of changed files could be erased.\"

(28) The Carnivore version reviewed by IITRI (Carnivore 1.3.4.) did not possess the ability to automatically record all of this information. *See supra* 26.

(29) For more details *see* http://www.cbc.ca/news/indepth/targetterrorism/backgrounders/moussaoui_zacarias.html and http://www.wsws.org/articles/2002/jan2002/mous-j05.shtml

(30) An internal memo leaked to the New York Times directly accuses Mueller and his aides of skewing, downplaying and mischaracterizing facts to avoid personal and institutional embarrassment and for political reasons. For more, *see* Julian Borger, *Agent accuses FBI of 'sabotage\'*, The Guardian, May 28, 2002 and Julian Borger, *FBI Chiefs blocked investigation of '20th hijacker\'*, The Guardian, May 25, 2002.

(31) *See* Ed Vulliamy, *A bad call?* The Observer, May 19, 2002 and Matthew Engel, *Bush warned of hijacks before*

September 11, The Guardian, May 17, 2002.

(32) The bureau has been struggling with computers that are over a decade old and incapable of even sending photographs over the internet.

(33) Article 21 of the Indian Constitution reads: \"No person shall be deprived of his life or personal liberty except according to procedure established by law.\"

(34) Article 19(1)(a) states: \"All citizens shall have the right to freedom of speech and expression.\"

(35) For example, *see People\'s Union for Civil Liberties v. Union of India*, A.I.R. 1997 SC 568, which dealt with the issue of telephone tapping, and could be broadly interpreted even in the context of the internet. *Kharak Singh v. State of U.P.*, A.I.R. 1963 SC 1295, *Gobind v. State of M.P.*, A.I.R. 1975 SC 137, and *Malak Singh v. State of P&H*, (1981) 1 SCC 420, are earlier cases decided by the Supreme Court of India interpreting the right to privacy in the context of police surveillance.

(36) Justice Holmes, in Dissenting opinion *Abrams v. United States*, 250 U.S. 616, 40 S.Ct. 17, 63 L.Ed. 1173 (1919).

(37) Nancy Chang, *What\'s So Patriotic About Trampling on the Bill of Rights?*, excerpt from Silencing Political Dissent: How Post-September 11 Antiterrorism Measures Threaten Our Civil Liberties (2002).

(38) The Nixon administration also sought to chill First Amendment political speech with harassment of high-profile dissidents from Martin Luther King, Jr. to John Lennon. The FBI, CIA and NSA have in the past compiled massive files on activities protected by the First Amendment. *See* Americo R. Cinquegrana, *supra* 17.

(39) *See* Sharon H. Rackow, *supra* 15.

(40) For a list of proscribed ‘terrorist organizations\' *see* U.S. Department of State Fact Sheet dated March 27, 2002, available at http://www.state.gov/s/ct/rls/fs/2002/9014.htm

(41) United States Department of State, *Patterns of Global Terrorism 2000*, Introduction (April 2001).

(42) Under this broad definition, it is possible that an immigrant who grabs a makeshift weapon in a sudden scuffle may be subject to removal as a \"terrorist\".

(43) In such cases, it is the non-citizen who is saddled with the difficult task of proving that his/her assistance was not intended to further terrorism.

(44) Currently, 29 organizations have been banned under the Act. *See* Indian Ministry of Home Affairs Press Release dated June 27, 2002, available at http://pib.nic.in/archieve/lreleng/lyr2002/rjun2002/27062002/r270620022.html

(45) *See supra* Sec. 3(1) of POTA defining ‘terrorist act\'.
(46) *See supra* Sec 802 of the PATRIOT Act defining ‘domestic terrorism\'.

(47) London-born Ahmed Omar Saeed Sheikh has been sentenced to death for abducting and murdering U.S. journalist Daniel Pearl. For a profile *see* Simon Jeffery, *Omar Sheikh (Special Report)*, The Guardian, July 15, 2002. For an interesting interview *see* http://news.bbc.co.uk/1/hi/world/south_asia/1806001.stm. *See also* Dexter Filkins, *Four in Pearl Murder are found Guilty in Pakistan Court*, New York Times, July 15, 2002.

(48) A Frenchman of Moroccan descent, Moussaoui is alleged to be the \"20th hijacker\" and has been indicted for conspiring with Osama bin Laden in the September 11 attacks. *See supra* 27 and 28. For an update on his trial *see* http://crime.about.com/library/weekly/aa20thHijacker.htm

(49) London-born Richard Reid, dubbed the ‘shoe-bomber,\' is facing trial in the U.S. for allegedly trying to blow up American Airlines flight 63 from Paris to Miami on December 22, 2001. Reid was subdued by passengers when he tried to ignite his sneakers. Reid attended the same mosque in London as Moussaoui, and is believed to have had contact with al-Qaida members. For a profile *see* http://news.bbc.co.uk/1/hi/uk/1731568.stm and for an update on his trial see http://crime.about.com/library/weekly/aasneakers.htm

(50) The present UK Terrorism Act, 2000 is permanent and not subject to routine review. Some of its provisions echo those of POTA and the PATRIOT Act. For instance, once an organization is proscribed by the Home Secretary, it is illegal to belong to it, support it financially, or even to be present at a meeting of three people or more if one of these

people is a member. While terrorism used to be defined as violence with political motivation, the Act widens the ambit to include anyone serving a \"political, *religious or ideological*\" cause, who uses violence or the threat of violence against people or property.

(51) Pervasive electronic surveillance and security checks have become a part of everyday life. In a major departure from long-established legal principle, a presumption of guilt could attach to an accused\'s decision to remain silent. Warrant-less searches, the muzzling of the electronic media, and restrictions on freedom of movement are all costs of Britain\'s response to terrorism.

(52) Ian Cuthbertson, *Whittling Liberties: Britain\'s not-so-temporary antiterrorism laws*, World Policy Journal, Winter 2001/2002.

(53) *Ibid*.

(54) *See* Donald Rumsfeld, *A War Like No Other Our Nation Has Faced*, The Guardian, September 28, 2001 and Leader, A Perilous Proposition, The Guardian, September 19, 2001. *See also* Michael Elliott, *We Will Not Fail*, Time magazine, October 1, 2001.

(55) David Cole, *Operating Enduring Liberty*, The Nation, June 3, 2002.

(56) Nicholas N. Kittrie, *Rebels With A Cause: The Minds and Morality of Political Offenders* (2000).

(57) *See generally* Philip B. Heymann, *Terrorism and America*, pp.100-103, 113-114 (1998).