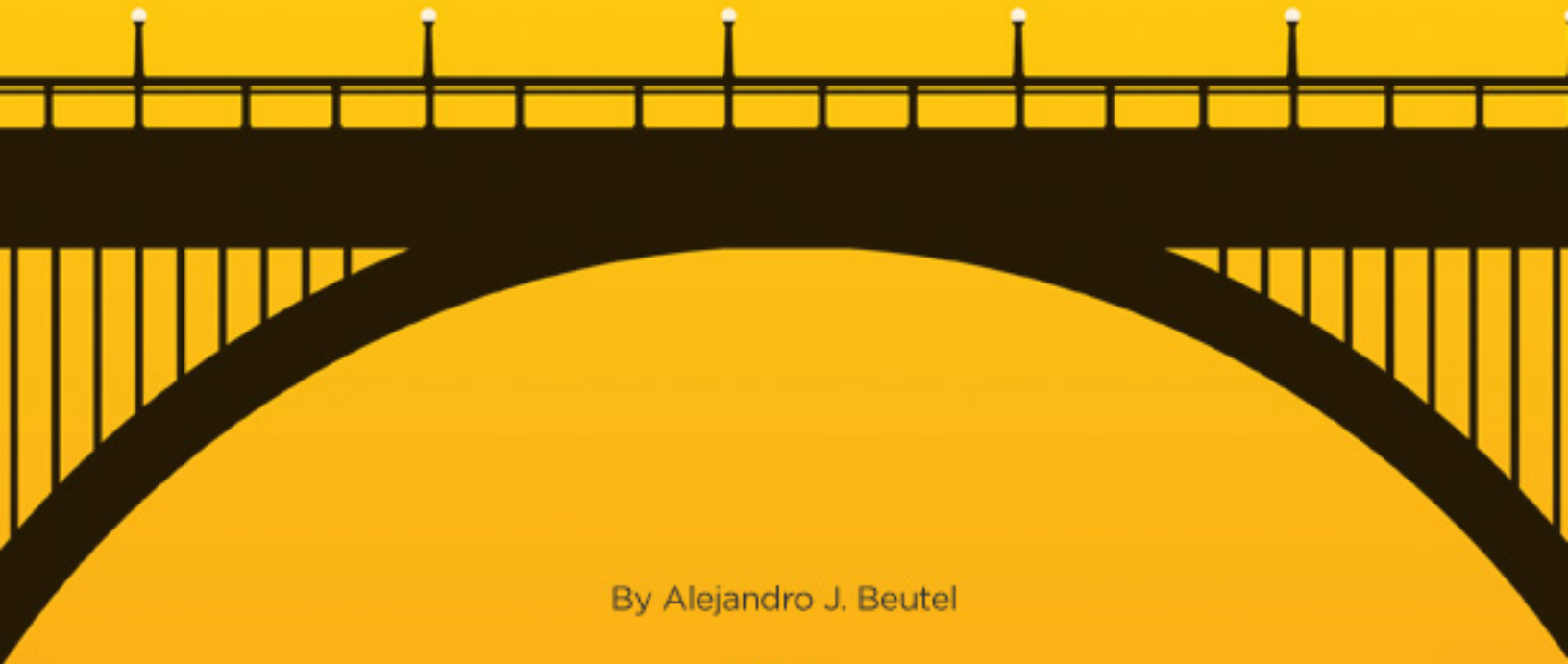
Building Bridges
TO STRENGTHEN AMERICA

FORGING AN EFFECTIVE COUNTERTERRORISM ENTERPRISE
BETWEEN MUSLIM AMERICANS & LAW ENFORCEMENT



By Alejandro J. Beutel

PART 4
CURRENT DOMESTIC COUNTERTERRORISM POLICIES

Muslim Public Affairs Council

Making Muslims part of the solution since 1988
WWW.MPAC.ORG

Current Domestic Counterterrorism Policies

We take a case-study approach, specifically analyzing some of the surveillance strategies being used to prevent terrorism. We review the widespread use of National Security Letters and Section 215 of the USA PATRIOT Act, the NSA warrantless surveillance, the under-regulation and overuse of informants, and racial profiling.

These four cases are selected because are used largely in the name of counterterrorism. They are also chosen because civil liberties groups have questioned the invasive nature and legal standing of these actions.

National Security Letters and Section 215 of the USA PATRIOT Act

National Security Letters (NSLs) can be described as a special kind of administrative subpoena used by the FBI and other security agencies to "seek customer and consumer transaction information in national security investigations from communications providers, financial institutions, and credit agencies."[1] Prior to 9/11, NSL statutes were carved out of a number of privacy laws that specified what kind of information could be obtained, under what circumstances it could be obtained and who it could be shared with.

These restrictions included:[2]

- Communications records, financial business records, credit agency records (all under limited circumstances) and the ability to use an NSL relating to an illegal release of classified information
- Only a select few individuals at FBI headquarters (FBIHQ) in Washington DC could sign off on an NSL
- The FBI needed "specific and articulable facts" about the target to request and/or obtain a letter
- The *primary* purpose of the investigation is to get information about "a foreign power or agent of a foreign power" (as defined by the FISA Act of 1978)
- Various other privacy statutes including the National Security Act and the Fair Credit Reporting Act contain restrictions on disseminating information

However after the 9/11 attacks took place, the USA PATRIOT Act changed these standards to allow NSL authority to be employed faster and wider. Under Section 505 of the Act, these changes included:[3]

- Expanded authority to issue NSLs beyond FBI Headquarters, to now include the heads of FBI field offices

- Changed the requirement from making the primary purpose of an investigation to seek information about "a foreign power or agent of a foreign power," to requiring that the NSL merely be "relevant" to an investigation

Subsection 358(g) of USA PATRIOT Act included a fifth NSL statute, by amending the Fair Credit Reporting Act to allow investigators to obtain consumer report records. Furthermore it allowed consumer reports to be provided, "…to any government agency investigating or analyzing international terrorism [or counterintelligence activities]…" in addition to the FBI.[4] This potentially allows agencies normally focused on foreign intelligence gathering, such as the CIA, to engage in certain aspects of domestic information collection.

Aside from the important question of the civil liberties and privacy impact of expanded NSL authority, we seek to examine the tool's effectiveness. Two reports from the Office of the Inspector General (OIG) within the Department of Justice can help answer the question. Overall, the OIG reports found a series of abuses and mistakes that contributed very little to counterterrorism efforts. (Both reports do not cover NSL use under Subsection 358(g) of the USA PATRIOT Act, which could include additional agencies like the CIA, NSA and DIA.)

According to the first report, published in March 2007,[5] there were at least 143,074 NSL requests during 2003-2005. The report is full of quoted and paraphrased statements from FBI investigators discussing the importance of Bureau's expanded powers, however the report's hard statistics paint a different picture. Out of the 143,074 NSL requests, only 153 legal proceedings emerged. Out of these 153 proceedings, only 1 request contributed to a "material support" for terrorism conviction. The report failed to mention how the NSL contributed in that particular case and it failed to mention its effectiveness in preventing any actual terrorist plot.

A second report from the Department of Justice OIG in March 2008, regarding Section 215 investigations – the so-called "library records" provision and an investigatory tool with powers similar to NSLs[6] – found their use in counterterrorism investigations to be ineffective. Most of the records obtained under Section 215 led to dead-ends.[7] It found that Section 215 requests were "an impractical tool because of the lengthy time involved in developing, reviewing and presenting the requests."[8] The delays in processing the requests were attributed to bureaucratic inefficiencies. **This finding is extremely important considering that a recently declassified monograph from the 9/11 Commission,[9] as well writings by FBI whistleblowers also point to long-standing bureaucratic inefficiencies as the principle cause for intelligence failures behind 9/11.**[10]

The report went on to note that other tools such as NSLs, grand jury subpoenas and an open source search "through public sources such as Google" were faster than Section 215 requests.[11] However as noted earlier, NSLs are also inefficient and ineffective. Grand jury subpoenas may be limited by a "criminal nexus",[12] however this point is moot since terrorism is considered a crime under US federal law[13] (and state laws)[14] and typically involves several precursor crimes[15] before an attack can be launched.

Both the March 2007 and March 2008 OIG reports show how the NSL and Section 215 tools were ineffective in counterterrorism investigations. The information overwhelmed analysts, as was the case with the National Security Letters, or it was too slow, as was the problem with Section 215 requests. Both cases divert limited resources from time-tested, efficient and effective investigative work. Instead FBI agents engaged in fishing expeditions for people's private information. This leaves one wondering whether or not such successes were worth the price paid in civil liberties and diverted resources.

NSA Wiretapping

In December 2005, the *New York Times* revealed that President Bush had authorized monitoring of communications of thousands of people between the United States and other countries without warrants.[16] Six months later, the *USA Today* revealed later monitoring also included purely domestic calls and has been trying to create a massive database of every call made within the US.[17] In addition to the legal aspects of the authorization, both of these news reports dealt with the National Security Agency's focus on signals intelligence, (SIGINT),[18] and how it contributes to national security. Though a legislative remedy with weaker civil liberties protections was passed in 2008,[19] in April 2009 the *New York Times* reported the NSA overstepped its legal authority and drastically "overcollected" U.S. domestic communications.[20]

Without delving into the legal analysis, serious questions about the policy's effectiveness, and more broadly the general role of wiretapping in counterterrorism efforts, need to be raised. Though government officials have publicly tried to show how the NSA warrantless wiretapping prevented terrorist attacks against the U.S., there has been little evidence of its effectiveness.

The role in which wiretapping can contribute to counterterrorism operations seem to be misplaced, disregarding certain tactical countermeasures terrorists have employed to avoid surveillance. As early as October 2002, a *USA Today* investigation found the NSA had trouble tracking Al-Qaeda operatives. Terrorist suspects were successfully evading U.S. surveillance "chiefly by using disposable cell phone or by avoiding phones altogether and substituting human messengers and face-to-face meetings to convey orders."[21] More recent news reports also indicate messages were sent through email.[22]

However, even on those rare occasions when the NSA or some other security agency manages to intercept a message, determining whether it has any tactical value or not is very difficult. In addition to the language barrier, the content of these messages are vague statements that can be easily misinterpreted.[23] Writing in the peer-reviewed academic journal *Intelligence and National Security*, surveillance expert Niels Sorells, notes:[24]

> This renders the government's ability to derive useful tips from such communications more or less moot… Intercepting a transmission is useless if so much gobbledygook is used that the conversation is meaningless to anyone without a key or would require so much time to decipher that the operation being discussed is likely to have been carried out by the time the message is decoded. The situation gets worse if there is not even a specific party to target.

Another problem with the NSA program is that it is ill-suited to deal with organizational adaptations to their changed operational environment. A 2006 *USA Today* investigation reported the NSA domestic spying efforts were producing data used for "social network analysis". Current social network analysis methods to guide SIGINT collection and analysis of information is called "snowball sampling."

According to a study jointly funded by the National Science Foundation, Office of Naval Analysis, and the Department of Defense, social network analysis and snowball sampling are effective against centralized and hierarchical organizations. However the same study found these techniques to be ineffective against decentralized "cellular" clusters of loosely connected individuals[25] - Al-Qaeda's now-preferred organizational setup.[26]Investigative media reports[27] and an official unclassified report from five Offices of the Inspector General (OIG 5)[28] also indicate that the NSA's massive domestic wiretapping program has been ineffective.

Yet one should not take this criticism as entirely dismissing the importance of wiretaps altogether; they can play an extremely important role. However past counterterrorism successes show that wiretaps must be conducted with the coordination and input of other types of intelligence.

Wiretapping is most effective when pieced together with findings from other types of information. In pointing to a successful operation in Germany against clandestine Al-Qaeda operatives that involved electronic surveillance combined with gains from human assets, Niels Sorrells further notes:[29]

> …much of the information was gathered by tracking phone records, not tapping phone lines. The authorities ascertained who was calling whom and then cross-referenced that data with information about criminal records and immigration violations before closing in. This is detective work, not randomly listening in hoping to hear something useful. It did not rely upon subjecting private citizens to official eavesdropping of their private conversations and communications.

The United States has its own example where different sources of intelligence, working together, allowed for a major bust against terrorists. As a *New York Times* investigation found, Khalid Shaikh Mohammed was arrested due to his own sloppiness for reusing the same SIM card in his cellular phones, making it easier for authorities to eventually track him down. Yet Mohammed's arrest would not have been possible without first investigating another Al-Qaeda militant, Christian Ganczarski. German police searched Ganczarski's house and found a journal with several phone numbers, including one that was used to track down Khalid Sheikh Mohammed in Pakistan and other Al-Qaeda suspects.[30]

The released OIG 5 report noted that law enforcement agents and intelligence analysts regarded the NSA spying as "…one source among many available analytic and intelligence-gathering tools in these efforts."[31] In the context provided earlier, the OIG 5 account appears to point toward both the ineffectiveness of the warrantless wiretapping, and the centrality of old-fashioned detective work in apprehending terrorist criminals.

Racial Profiling

Racial profiling is an important counterterrorism policy concern that occurs in many different contexts. In some cases, it can take place while a person is engaged in routine activities such as travel, work or worship. Other cases are alarmingly more sophisticated, such as the Los Angeles Police Department's failed attempt to "map" Muslim communities in the L.A.-metropolitan area[32] and concerns that the FBI may be permitting "mapping of ethnic minority groups for a variety of reasons."[33]

Though most reported cases of racial profiling by law enforcement appear to take place at the local and state levels,[34] it is also an issue of concern for various ethnic and civil liberties groups at the federal level. Although the Department of Justice issued a June 2003 guidance document on the use of race in law enforcement, it has several exceptions to it, including in national security investigations and intelligence activities.[35] In addition, news reports have cited the concerns of many civil liberties groups over the latest revisions to the Attorney General's guidelines on initiating domestic counterterrorism investigations. Such concerns are largely focused on the reduction of legal standards to initiate an investigation. One of the most troubling aspects is the legal power it gives law enforcement to initiate an investigation based on racial and religious profiling.[36]

However, there are also important security policy reasons to be concerned over racial profiling. Muslim American communities tend to be extremely diverse, reflecting the racial, ethnic and cultural pluralism of the larger global Muslim community. This includes South Asians, Southeast Asians, Arabs, Sub-Saharan Africans and larger numbers of "indigenous" African American, Caucasian and Latino Muslim Americans.

How can one tell who is Muslim and who is not? One may try by looking at a person's name. However, there really is no such thing as what may be popularly thought of as a "Muslim" name – mostly it is an Arabic name. Things are further complicated by the fact that two-thirds of all Arabs living in the United States are Christian, not Muslim.[37] In addition, there are many Muslim converts who do not legally change their names to Arabic-sounding names. Jose Padilla, John Walker Lindh, Michael Finton, Dhiren Barot, Colleen LaRose, and Richard Reid are prominent examples of Muslim violent extremists who fit this description.

If developing actionable information to prevent violent extremism can be compared to finding needles in a haystack, then racial profiling is merely adding more hay to the stack. In fact, statistics show that policies employing racial profiling have been unsuccessful. Three cases involving Muslim Americans are worth mentioning.

First were the mass arrests of people of Arab/Muslim descent immediately after 9/11. Between September 11, 2001 and September 2, 2004, then-Attorney General John Ashcroft aggressively detained 5,000 people. However none of them were ever convicted on terrorism charges.[38]

The second example was a Department of Homeland Security-led dragnet called "Operation Front Line." Months before, during and after the 2004 Presidential elections, law

enforcement officials arrested and detained over 2,000 people from Muslim-majority countries. Like the earlier mass arrests after 9/11, no one was ever convicted on charges of threatening national security or terrorism.[39]

The third example is the National Security Entry-Exit Registration System (NSEERS) program. After 9/11, the program mandated that over 83,000 "suspicious" individuals, overwhelmingly from Muslim-majority countries, had to notify the Department of Homeland Security of their whereabouts every 30 days. From this group, no terrorist convictions have emerged.[40]

The only other possible way of figuring out who is a Muslim and who is not is by their "religious" clothing. However not all Muslims dress "religiously," whatever that may mean. Furthermore violent extremists need to keep a low profile in order to maintain operational security before carrying out an attack. If Al-Qaeda members dressed "religiously," they would fit into stereotypes that would draw attention to them. In light of their concern for operational security, it is not surprising that the 9/11 hijackers all dressed like Westerners and some had shaved their beards. Therefore it makes little sense to profile based on appearance and/or clothing.

As research has shown, Al-Qaeda has sought to maximize its operational effectiveness by seeking recruits who can best blend into their host societies. This at least partly explains why so many Al-Qaeda terrorists come from relatively secular, Western-educated backgrounds (with little religious education).

Furthermore, reports indicate Al-Qaeda has sought to recruit from a variety of ethnic and racial backgrounds, including Caucasians.[41] Even Muslims from "traditional" ethnic backgrounds may try to change their external appearances so they can be perceived as a member of a traditionally non-Islamic ethnic background. One example is the case of convicted terrorism suspect Shahawar Matin Siraj, who dressed to "look hip-hop, like a Puerto Rican" and not "look Arabic."[42] In another instance, Al-Qaeda may simply use operatives from a different racial or ethnic background altogether to avoid specific physical profiles. The use of mostly Black East Africans in the failed 7/21 London attacks two weeks after the deadly 7/7 London operation by majority-South Asians is one such example.

In addition to being tactically ineffective, racial profiling is strategically counterproductive. The best sources of information needed to prevent terrorist attacks come from within communities where terrorists are hiding.[43] Profiling individuals based on their race, ethnicity and/or religion not only has a negative net impact on civil liberties and fails to unravel terrorist networks, it alienates the communities law enforcement needs to get actionable information to prevent future attacks. It also makes individuals and organizations become extremely reluctant to cooperate with law enforcement.[44]

Finally, racial profiling overlooks threats coming from other religio-ideological sources. As our database on post-9/11 incidents shows, Muslims are not the only serious source of counterterrorist concern. If racial profiling were more pervasive in law enforcement practices, many of those non-Muslim plots contained in our database may not have been prevented.

Informants

Informants are an extremely important tool and can be used to great effectiveness in various kinds of criminal investigations, including counterterrorism ones. According to Boston College Law Professor Robert Bloom, there are two types of informants: the "incidental informer" and the "confidential informer".[45] Others such as former FBI counterterrorism investigator William E. Dyson, divide informants into short-term and long-term categories.[46] Our review of informants focuses on long-term "confidential" sources, not short-term "incidental" sources.

The earliest recorded use of informants dates back to classical Athens, when they were employed to prevent treason against the state.[47] However history demonstrates that using informants can also be abused by the government for political purposes.[48]

Modern American policing has similar examples of legitimate and illegitimate uses of informants. The FBI has successfully used them against the organized crime syndicates such as various mafia crime bosses in the 1980s. However it has also abused them, such as the investigation, infiltration and instigation of radical but mostly non-violent groups under its Counterintelligence Program, or COINTELPRO, during the 1960s and 70s.[49]

A comparison between today's uses of informants by the FBI with their uses during COINTELPRO is important. The reason for doing this is not for the purposes of political polemics, but what appear to be strikingly similar policy directions. Prior to the exposure of COINTELPRO abuses by the Church and Pike Committees, there was virtually no internal or legislative regulation of FBI informants.[50]

As a response to public outcry and a means of avoiding direct legislative regulation of informants, Attorney General Edward Levi established the first set of internal guidelines for the use of informants in 1976. The key contribution of the guidelines was that the FBI needed to satisfy a "specific and articulable facts" standard of proof that an individual is involved in violent or potentially violent activities. This draws a fine line between what may be solicitation or intention to commit a crime, like terrorism, and otherwise Constitutionally-protected activities.

Problems with controlling informant activities continued, and the internal guidelines were updated and expanded as time went on to solve emerging issues. In 1983, Attorney General William Smith lowered the standard of proof to a "reasonable indication" requirement which remained constant until shortly after 9/11.[51]

Following 9/11, Attorney General John Ashcroft removed the "reasonable indication" standard altogether, allowing investigations without past reason for suspicion of criminal activity. As a result the thin line between Constitutionally-protected speech and criminal activity began to be blurred. Attorney General Michael Mukasey's November 2008 revisions to the guidelines went further by repealing five sets of guidelines on investigations and substituted them with one. While the Mukasey revisions reaffirm the Ashcroft revisions which allow spying at any public gathering without prior indication of criminal activity – including mosques and social service agencies/activities – they also permit racial profiling.

By allowing low to non-existent standards of proof, the Ashcroft and Mukasey revisions bear striking resemblance to the minimalist policies of the COINTELPRO-era FBI use of informants.[52]

MPAC's concern with the under-regulation of informants – as was the case during COINTELPRO – focuses on its negative policy effects to preventing terrorism. We leave the legal discussions of civil liberties and privacy impacts to others.

We do not argue that the use of informants should be discontinued altogether; they can serve as an effective and legitimate law enforcement tool to bring criminals to justice. Nevertheless, it also has its tactical limitations, and if used improperly, can be strategically counterproductive. This policy dilemma is worsened by the current overuse and under-regulation of informants.

One problem is that the overuse of informants will not provide better information on potential terrorist operations; instead *it will leave a critical intelligence gap*. Informants can be an extremely valuable tool against terrorism, but their utility is largely affected by the type of organizational structure a terrorist group adopts. Hierarchical "pyramid" organizations defined by their connected command and control structures, like the IRA and pre-9/11 Al-Qaeda, make themselves much more vulnerable to being compromised if penetrated by an outside agent or an internal informant. When that occurs, because the human intelligence asset is in regular contact with other terrorist group members, information on other personnel and activities can be gathered with relative ease.

However, a hierarchical structure is not the likely choice of operation for most domestic terrorists – Muslim or non-Muslim. Domestic terrorists are more likely to arrange themselves as autonomous cells to avoid widespread compromise of a violent extremist movement. Louis Beam, a White Supremacist and militant strategist who popularized the concept of "Leaderless Resistance" (a cellular method of violent extremism), explains why:[53]

> …Such a situation is an intelligence nightmare for a government intent upon knowing everything they possibly can about those who oppose them. The Federals, able to amass overwhelming strength of numbers, manpower, resources, intelligence gathering, and capability at any given time, need only a focal point to direct their anger. A single penetration of a pyramid type of organization can lead to the destruction of the whole. Whereas, Leaderless Resistance presents no single opportunity for the Federals to destroy a significant portion of the Resistance.

Another related problem is that informants – especially when they are under-regulated – are less likely to catch terrorists, particularly when they organize themselves along a cellular structure. Terrorists are trained to be very cautious about maintaining their security by developing training manuals and studying law enforcement manuals to know police surveillance techniques. As former FBI counterterrorism investigator William Dyson notes, "Spotting informants and identifying tactics employed by law enforcement officers to penetrate terrorist groups are often covered in security manuals."[54]

All of this assumes that informants are honest and will provide accurate information – which is frequently not the case. For instance, empirical studies based on data from exonerated

and/or released defendants, show informants very frequently provide incomplete or false information.[55]

Furthermore, the actions of informants may end up entrapping impressionable and radical but non-violent individuals who may not have otherwise been inclined to commit a crime. This could end up creating or at least encouraging more criminal activity. Many times, police will tolerate crimes by informants in order ensure they maintain their operational security and continue their intelligence collection. However this can undermine the overarching goal of increasing public security. During COINTELPRO, there were cases where informants had committed or incited acts of violence, with the tacit or even explicit approval of FBI handlers.[56] More recently, news surfaced that Hal Turner, a controversial Neo-Nazi blogger, was in fact an FBI informant who reported on Right-Wing violent extremists. Turner was eventually arrested, but only after 7 years of making statements that attempted to incite non-violent followers to commit acts of violence.[57]

Even if one were to assume the surveillance target had not been incited to commit a terrorist act – which is debatable in some recent cases –[58] it is more likely the types of people arrested as a result of ethically questionable actions of informants are incompetent individuals. If that is the case, it is highly unlikely they were needed to capture such low-skilled criminals. In fact, the arrests in most of the Muslim domestic violent extremism cases seem to indicate they were just that – impressionable and/or incompetent.[59]

While at least one notable study has detailed the institutional and communal ramifications of the pervasive use of informants,[60] their improper use can also present serious strategic concerns for law enforcement. Most notably, it can ruin the important relations between law enforcement and Muslim American communities. Muslim communities may be less willing to cooperate with law enforcement due to a sense of "betrayal" of a trusted partnership, especially if they perceive terrorism busts to be cases of entrapment. It also undermines the credibility of mainstream religious leaders who advocate for engagement with law enforcement. As a result, the cooperative relationship between law enforcement and Muslims is severely strained or completely undermined. Law enforcement will find it difficult to get important information needed to prevent a future terrorist attack,[61] thus leaving a critical intelligence gap that cannot be filled by other means including the overuse and under-regulation of informants.[62]

To be fair, informants at times can be effective in counterterrorism investigations even against cellular structures. Because terrorist groups are concerned about their operational security, fear of informants can create and increase tensions within a terrorist cell. As a result, it may generate enough paranoia that a cell may abandon a planned operation.

However, using informants against cellular structures will make less of an impact against a group of militants than if they were used against a network. Unlike connected networks, information and members are compartmentalized in cellular structures. Penetration of one cell is less likely to yield information on other potential violent extremists, rather than in a networked organization.[63]

This limited tactical benefit must be weighed against the larger strategic costs of using informants – especially when overused and underregulated. In order to achieve maximum effectiveness of informants, they will need to be used with along with other investigative techniques. Better legal mechanisms and internal guidelines need to be put in place to ensure their relevance to preventing actual criminal activity.

Finally, a more circumspect calculation by law enforcement agents should be made when considering employing informants: Are the gains of using an informant worth it if the short-term intelligence and prosecutorial benefits are limited but the long-term social and intelligence gathering costs from harmed community relations are high?

Endnotes

[1] Charles Doyle, "National Security Letters in Foreign Intelligence Investigations: A Glimpse of the Legal Background and Recent Amendments." *Congressional Research Service*, (March 28, 2008), P.1. Available at: http://www.fas.org/sgp/crs/intel/RS22406.pdf.
[2] Ibid., P. 2.
[3] Ibid., P. 3.
[4] Ibid., P. 3.
[5] Glenn Fine, "A Review of the Federal Bureau of Investigation's Use of National Security Letters." *Department of Justice Office of the Inspector General*, (March 2007). Available at: www.usdoj.gov/oig/special/s0703b/final.pdf. Also see: Mike German, "ACLU Roadmap of Justice Department Inspector General's Review of the FBI's Use of National Security Letters." *American Civil Liberties Union*, (March 19, 2007). Available at: http://www.aclu.org/safefree/nationalsecurityletters/29067leg20070319.html.
[6] "National Security Letters & Section 215 of the USA Patriot Act." *The Constitution Project*, (2009). Available at: http://2009transition.org/liberty-security/index.php?option=com_content&view=article&id=12&Itemid=22.
[7] Glenn Fine, "A Review of the FBI's Use of Section 215 Orders for Business Records in 2006." *Department of Justice Office of the Inspector General*, (March 2008), P. 52. Available at: http://www.usdoj.gov/oig/special/s0803a/final.pdf
[8] Ibid., P. 55.
[9] Barbara A. Grewe, "Legal Barriers to Information Sharing: The Erection of a Wall Between Intelligence and Law Enforcement Investigations." *Commission on Terrorist Attacks Upon the United States*, (August 20, 2004). Available at: http://www.fas.org/irp/eprint/wall.pdf.
[10] Mike German, "An Insider's Guide to the 9/11 Commission Report." *GlobalSecurity.org*, (2005). Available at: http://www.globalsecurity.org/security/library/report/2005/guide-iii.htm; Colleen Rowley, "Statement of Colleen M. Rowley, FBI Special Agent and Minneapolis Chief Division Counsel, Before the Senate Committee on the Judiciary 'Oversight Hearing on Counterterrorism.'" *United States Senate Committee on the Judiciary*, (June 6, 2002). Available at: http://www.fbi.gov/short/sacrstate.htm
[11] Fine, "A Review of the FBI's Use of Section 215 Orders," P. 55.
[12] Ibid., P. 56.
[13] See Title 28 Code of Federal Regulations Section 0.85: the unlawful use of force and violence against persona or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives."
[14] For instance, see: Donna Lyons, "States Enact New Terrorism Crimes and Penalties." *National Council for State Legislatures*, (November 2002). Available at: http://www.ncsl.org/Portals/1/documents/cj/terrorismcrimes.pdf.
[15] For an overview of terrorist precursor crimes, see: Siobhan O'Neil, "Terrorist Precursor Crimes: Issues and Options for Congress." *Congressional Research Service*, (May 24, 2007). Available at: http://www.fas.org/sgp/crs/terror/RL34014.pdf.
[16] James Risen and Eric Lichtblau, "Bush Lets U.S. Spy on Callers Without Courts." *New York Times*, (December 16, 2005). Available at: http://www.commondreams.org/headlines05/1216-01.htm.
[17] Leslie Cauley, "NSA Has Database of Americans' Phone Calls." *USA Today*, (Msy 11, 2006). Available at: http://www.usatoday.com/news/washington/2006-05-10-nsa_x.htm.
[18] Daniel Smith, "Background on the Role of Intelligence in Rooting out Terrorism." *Center for Defense Information*, (September 14, 2001). Available at: http://www.cdi.org/terrorism/intelligence-role.html

[19] Pamela Hess, "Senate Immunizes Telecom Firms from Wiretap Lawsuits." *Associated Press*, (July 9, 2008). Available at: http://www.nysun.com/national/senate-grants-telecom-companies-immunity/81525/.
[20] Eric Lichtblau and James Risen, "Officials say U.S. Wiretaps Exceeded Law." *New York Times*, (April 15, 2009). Available at: http://www.nytimes.com/2009/04/16/us/16nsa.html?pagewanted=all
[21] John Diamond, "Al-Qaeda Steers Clear of NSA's Ears." *USA Today*, (October 17, 2002). Available at: http://www.usatoday.com/news/washington/2002-10-17-nsa-al-qaeda_x.htm
[22] Pamela Hess, "Al-Qaida Used Hotmail, Simple Codes in Planning." *Associated Press*, (May 1, 2009). http://www.newsvine.com/_news/2009/05/01/2762579-al-qaida-used-hotmail-simple-codes-in-planning
[23] Diamond, "Al-Qaeda Steers Clear".
[24] Niels C. Sorrells, "Taps and Terrorism: A German Approach?" *Intelligence and National Security*, Vol. 23, No. 2, (April 2008), P. 188-89.
[25] Maksim Tsvetovat and Kathleen M. Carley, "On Effectiveness of Wiretap Programs in Mapping Social Networks." *Paper Presented at 2006 SIAM Conference on Data Mining*, (April 20-22,2006), P. 1. Available at: http://www.siam.org/meetings/sdm06/workproceed/Link%20Analysis/23netwatch_link_analysis_BW.pdf
[26] For instance see: Brynjar Lia, "Al-Suri's Doctrines for Decentralized Jihadi Training – Part 1." *Jamestown Foundation Terrorism Monitor*, Vol. 5, No. 1, (January 18, 2007), P. 1-3; Brynjar Lia, "Al-Suri's Doctrines for Decentralized Jihadi Training – Part 2." *Jamestown Foundation Terrorism Monitor*, Vol. 5, No. 2, (February 1, 2007), P. 1-3.
[27] Lowell Bergman, Eric Lichtblau, Scott Shane and Don Van Natta Jr., "Spy Agency Data After Sept. 11 Led F.B.I. to Dead Ends." *New York Times*, (January 17, 2006). Available at: http://www.nytimes.com/2006/01/17/politics/17spy.html; Barton Gellman, Dafna Linzer and Carol D. Leonning, "Surveillance Net Yields Few Suspects." *Washington Post*, (February 5, 2006). Available at: http://www.washingtonpost.com/wp-dyn/content/article/2006/02/04/AR2006020401373.html.
[28] "Unclassified Report on the President's Surveillance Program." *Offices of Inspectors General of the Department of Defense, Department of Justice, Central Intelligence Agency, National Security Agency, Office of the Director of National Intelligence*, (July 10, 2009). Available at: http://www.fas.org/irp/eprint/psp.pdf.
[29] Sorrells, "Taps and Terrorism", P. 189.
[30] Don Van Natta Jr. and Desmond Butler, "How Tiny Swiss Cellphone Chips Helped Track Global Terror Web." *New York Times*, (March 4, 2004). Available at: http://www.nytimes.com/2004/03/04/international/europe/04PHON.html?pagewanted=all.
[31] "Unclassified Report on the President's Surveillance Program," P. 38.
[32] Jill Serjeant, "L.A. Police Drop Controversial Muslim Mapping Plan." *Reuters*, (November 15, 2007). Available at: http://www.reuters.com/article/idUSN1560353720071115.
[33] "Muslim Advocates Lawsuit Seeks FBI Surveillance Guidelines Charities and Mosques." *Charity and Security Network*, (September 30, 2009). Available at: http://www.charityandsecurity.org/news/Muslim_Advocates_Lawsuit_Seeks_FBI_Surveillance_Guidelines_Charities_Mosques.
[34] See: "Threat and Humiliation: Racial Profiling, Domestic Security and Human Rights in the United States." *Amnesty International*, (October 2004). Available at: http://www.amnestyusa.org/racial_profiling/report/rp_report.pdf.
[35] See: "Guidance Regarding the Use of Race by Federal Law Enforcement Agencies." *Department of Justice Civil Rights Division*, (June 2003). Available at: http://www.justice.gov/crt/split/documents/guidance_on_race.php.
[36] See: "Muslim Advocates v. United States Department of Justice." *Muslim Advocates*, (September 16, 2009). Available at:

http://www.muslimadvocates.org/documents/Muslim%20Advocates%20Complaint%20To%20File.pdf; Director Defends FBI Over Test Cheating Allegations." *Associated Press*, (July 28, 2010). Available at: http://www.npr.org/templates/story/story.php?storyId=128824851&ft=1&f=1003.

[37] Based on statistics from the 2002 Zogby International Survey of Arab Americans' religious affiliations. See: "Demographics." *Arab American Institute*, (2009). Available at: http://www.aaiusa.org/arab-americans/22/demographics.

[38] David Cole, "Taking Liberties." *The Nation*, (September 16, 2004). Available at: http://www.thenation.com/doc/20041004/cole

[39] Eric Lichtblau, "Inquiry Targeted 2,000 Foreign Muslims in 2004." *New York Times*, (October 30, 2008). Available at: http://www.nytimes.com/2008/10/31/us/31inquire.html. Also see: "ICE Targets Immigrants from Muslim Majority Countries Prior to 2004 Election." *Arab-American Anti-Discrimination Committee* and *Yale Law School*, (October 20, 2008). Available at: http://www.adc.org/PDF/frontline.pdf.

[40] David Cole and Jules Lobel, "Are We Safer?: A Report Card on the War on Terror." *Los Angeles Times*, (November 18, 2007). Available at: http://www.latimes.com/media/acrobat/2007-11/33860990.pdf.

[41] Hayder Mili, "Al-Qaeda's Caucasian Foot Soldiers." *Jamestown Foundation Terrorism Monitor*, Vol. 4, No. 21, (November 2, 2006). Available at: http://www.jamestown.org/programs/gta/single/?tx_ttnews%5Btt_news%5D=948&tx_ttnews%5BbackPid%5D=181&no_cache=1.

[42] Craig Horowitz, "Anatomy of a Foiled Plot." *New Yorker Magazine*, (November 29, 2004). Available at: http://nymag.com/nymetro/news/features/10559/.

[43] For instance see: Guy Taylor and Jon Ward, "Muslims Seen as Asset in War on Terror." *Washington Times*, (November 10, 2004).

[44] Daphne Evitar, "New Surveillance Rules Threaten FBI Relationship With Muslim Groups." *Washington Independent*, (May 5, 2009). Available at: http://washingtonindependent.com/41861/new-surveillance-rules-threaten-fbi-relationship-with-muslim-groups; "In Terror War, American 'outreach' has US Muslims Weary." *Reuters*, (May 9, 2006).

[45] Robert M. Bloom, "A Historical Overview of Informants." *Boston College Law School*, (March 16, 2005), P. 1.

[46] William E. Dyson, *Terrorism: An Investigator's Handbook*. 2nd ed. (Albany, NY: Matthew Bender Inc.), P. 170-71.

[47] Bloom, "A Historical Overview of Informants," P. 3.

[48] Ibid., P. 7, 10.

[49] Ibid., P. 11.

[50] "The Federal Bureau of Investigation's Compliance with the Attorney General's Investigative Guidelines." *Department of Justice Office of the Inspector General*, (September 2005), P. 31-36.

[51] Ibid., P. 36-61.

[52] "An Erosion of Civil Liberties." *New York Times*, (May 31, 2002). Available at: http://www.nytimes.com/2002/05/31/opinion/31FRI2.html; Nat Hentoff, "The Terror of Pre-Crime." *The Progressive*, (September 2002). Available at: http://www.ratical.org/ratville/CAH/preCrimeTerr.pdf; Shahid Buttar, "The Return of COINTELPRO: Government Infiltration of Activist Groups." *American Constitution Society Blog*, (September 4, 2009). Available at: http://www.acslaw.org/node/14047; G.W. Schulz, "Broader FBI Powers Now Set in Stone." *Center for Investigative Reporting*, (October 6, 2008). Available at: http://www.centerforinvestigativereporting.org/blogpost/20081006broaderfbipowersnowsetinstone; "The Attorney General's Guidelines." *Electronic Privacy Information Center*, (2008). Available at: http://epic.org/privacy/fbi/.

[53] Beam, "Leaderless Resistance"

[54] Dyson, *Terrorism: An Investigator's Handbook*, P. 62.

[55] Robert P. Mosteller, "The Special Threat of Informants to the Innocent Who Are Innocents: Producing 'First Drafts,' Recording Incentives and Taking a Fresh Look at the Evidence." *Ohio State Journal of Criminal Law*, Vol. 6, (2009), P. 549-551.
[56] German, *Thinking Like a Terrorist*, P. 59-68.
[57] David Owens, "Lawyer: FBI Trained Hal Turner as an 'Agent Provocateur." *Hartford Courant*, (August 18, 2009). Available at: http://www.courant.com/news/politics/hc-web-hal-turner-0819aug19,0,1700724.story; Natasha Korecki, "Man Accused of Threatening Judges was a Paid Informant for the FBI." *Chicago Sun-Times*, (August 11, 2009). Available at: http://www.suntimes.com/news/24-7/1709890,CST-NWS-blogger11.article.
[58] Cases that come to mind include the Sears Plot Tower Seven, the Newburgh Four, the Fort Dix Six and the JFK Four.
[59] Bruce Schneier, "Portrait of the Modern Terrorist as an Idiot." *Wired.com*, (June 14, 2007). Available at: http://www.wired.com/politics/security/commentary/securitymatters/2007/06/securitymatters_0614; Bruce Schneier, "This Week's Terrorism Arrests." *Schneier.com*, (May 22, 2009). Available at: http://www.schneier.com/blog/archives/2009/05/this_weeks_terr.html; Bruce Rushton, "Entrapment Defense Possible for Accused Bomber, but Likely Loser, Experts Say." *GateHouse News Service*, (September 25, 2009). http://www.galesburg.com/news/news_state/x576523952/Entrapment-defense-possible-for-accused-bomber-but-likely-loser-experts-say.
[60] Alexandra Natapoff, "Snitching: The Institutional and Communal Consequences." *University of Cincinnati Law Review*, Vol. 73, (2004), P. 645-702.
[61] David A. Harris, "Law Enforcement and Intelligence Gathering in Muslim and Immigrant Communities After 9/11." *University of Pittsburgh School of Law*, (January 2009).
[62] Martin Innes, "Policing Uncertainty: Countering Terror through Community Intelligence and Democratic Policing." *Annals of the American Academy*, (May 2006), P. 9, 11.
[63] Innes, "Policing Uncertainty," P. 10-11.

Founded in 1988, MPAC is an American institution which informs and shapes public opinion and policy by serving as a trusted resource to decision makers in government, media and policy institutions. MPAC is also committed to developing leaders with the purpose of enhancing the political and civic participation of Muslim Americans.

WASHINGTON, D.C.
110 Maryland Ave. N.E. Suite 210
Washington, D.C. 20002
Tel: (202) 547-7701
Fax: (202) 547-7704

LOS ANGELES
3010 Wilshire Blvd. #217
Los Angeles, CA 90010
Tel: (213) 383-3443
Fax: (213) 383-9674

WWW.MPAC.ORG