WORKING DRAFT
Contact author before citing

Predictive Analytics: The Use and Constitutionality of Technology in Combating Homegrown Terrorist Threats

Rajbir Singh Datta

CONTENTS

Predictive Analytics: The Use and Constitutionality of Technology in Combatting Homegrown Terrorist Threats

Rajbir Singh Datta[1]

I. INTRODUCTION.

On April 15, 2013 at approximately 2:50 p.m. as runners completed their journey through the Boston Marathon, two explosions occurred, ten to fifteen seconds apart and 550 feet away from each other, killing three and injuring over 170 innocent Americans.[2] As volunteers, runners, bystanders and emergency personnel risked their lives to aid the injured, no one knew if other explosions were imminent. The improvised explosive devices ("IEDs") were made of pressure cookers containing nails, ball bearings, and other shrapnel, combined with an electronic detonator.[3] The bombs were designed not to kill, but to severely maim innocent bystanders as they watched the race.[4]

As the forensics investigation continued, many leads have been generated, and many have been discounted, with disturbing results.[5] State officials reported there were no intelligence assessments revealing credible threats in Boston prior to the attack.[6] On April 18, 2013, the FBI released images of two suspects who were later identified as brothers Tamerlan and Dzhohkar Tsarnev, 26 and 19, respectively.[7] On April 19, 2013, prior to engaging in a firefight and hurling explosive devices against police, resulting in the injury of a Transit police officer, the pair killed a Massachusetts Institute of Technology campus police officer.[8] Tamerlan Tsarnev was shot and killed during the firefight with police and his younger brother was barricaded, and eventually turned himself in after being wounded and barricading himself in a boat in Watertown, Massachusetts.[9]

[1] J.D., 2013, Earle Mack School of Law at Drexel University; M.P.A., American University; B.A., Temple University. Former National Director, Sikh American Legal Defense and Education Fund (SALDEF).

[2] *See Site of the Explosions at the Boston Marathon*, New York Times (Apr. 15, 2013), http://www.nytimes.com/interactive/2013/04/15/us/site-of-the-boston-marathon-explosion.html; Jeff Black, *Timeline: Tragedy at the Boston Marathon*, (Apr. 15, 2013), http://usnews.nbcnews.com/_news/2013/04/15/17767941-timeline-tragedy-at-the-boston-marathon?lite.

[3] Katherine Q. Seelye, Eric Schmitt and Scott Shane, *Boston Bombs Were Loaded to Maim*, New York Times (Apr. 16, 2013), http://www.nytimes.com/2013/04/17/us/officials-investigate-boston-explosions.html?pagewanted=all&_r=0.

[4] *Id.*

[5] *See* Amy Davidson, *The Saudi Marathon Man*, The New Yorker (April 17, 2013), www.newyorker.com/online/blogs/comment/2013/04/the-saudi-marathon-man.html.

[6] *See* Josh Levs and Monte Plott, *Boy, 8, one of 3 Killed in Bombings at Boston Marathon; Scores Wounded*, CNN (Apr. 18, 2013), http://www.cnn.com/2013/04/15/us/boston-marathon-explosions.

[7] Pete Williams, Richard Esposito, Michael Isikoff, and Eric McClam, *One Boston Marathon Suspect Killed; Second Suspect, his Brother, on Loose After Firefight*, NBC News (April 19, 2013), http://usnews.nbcnews.com/_news/2013/04/19/17817173-one-boston-marathon-suspect-killed-second-suspect-his-brother-on-loose-after-firefight?lite.

[8] *Id.*

[9] *Id.*

As the terror investigation continues it has been revealed that the brothers were born and raised in Russia and may have had ties to Chechnya where Muslim radicalism has been rampant.[10] According to public photos on the internet documenting the older brother's training for the Golden Gloves Boxing Competition, the pair fled to Kazakhstan in the 1990s to escape the violence in Chechnya before making their way to the United States as refugees.[11] The photo captions also quote Tamerlan as saying, "I don't have a single American friend. I don't understand them."[12] The pair have been in the United States since 2002 and the younger brother was a second-year medical student in the Boston area.[13] Although it is yet unclear the motivations behind the attack, it has been revealed that the older brother had posted on YouTube, video's discussing an Islamic prophecy frequently associated with al Qaeda.[14] Additionally, the Russian government allegedly revealed to the FBI concerns that Tamerlan Dzhokar was involved in extremist activities.[15] This led the FBI interviewing Tamerlan, performing a background check, running his name through relevant databases and checking on his communications and overseas travel.[16] However, the FBI missed the threat – there was no chatter, no intelligence revealing the Tamerlan's intentions.

The solution to this incident may, in the future, reside in the use of predictive analytics, which relies on capturing relationships between explanatory and predicted variables from past occurrences and exploiting them to predict future outcomes.[17] An algorithm would data mine through massive amounts of open source data, linking information about a potential suspect from multiple different sources and provide law enforcement with targets to further investigate. Therefore, using a predictive analytical algorithm, combined with open source information, and information from traditional intelligence and law enforcement mechanisms, may allow the security apparatus to predict future outcomes. However, despite the national security implications, such a program would require access to massive amounts of data that would need to be stored. It would also complicate the privacy and legal regime that the law has in currently in place.

The purpose of this paper is to discuss the use, legal implications, and challenges of utilizing predictive analytics as a tool to enhance intelligence and law enforcement communities with their efforts to combat homegrown extremism. This

[10] Eileen Sullivan, Meghan Barr and Katie Zezima, *1 of 2 Suspects in Boston Bombing Killed*, AP (Apr. 19, 2013), http://bigstory.ap.org/article/police-converge-neighborhood-outside-boston.
[11] *Will Box for Passport*, http://johanneshirn.photoshelter.com/gallery/-/G0000VQW7v6xWA7o/. Last Accessed April 19, 2013.
[12] *Id.*
[13] *Id.*
[14] Kevin Robillard, *Reports: Boston Bombing Suspects Came From Abroad*, POLITICO (Apr. 19, 2013), http://www.politico.com/story/2013/04/report-boston-bombings-suspects-abroad-90323.html.
[15] *See FBI Interviews Dead Boston Bombing Suspect Years Ago*, CBS News (Apr. 19, 2013), http://www.cbsnews.com/8301-201_162-57580534/fbi-interviewed-dead-boston-bombing-suspect-years-ago/.
[16] *Id.*
[17] *See Leveraging Data for International and External Threat Detection*, IBM, May 2010, at 1, located at http://public.dhe.ibm.com/common/ssi/ecm/en/ytw03044gben/YTW03044GBEN.PDF. Last visited March 19, 2013.

paper will not, as other papers on the subject of homegrown extremism, focus solely on the threat of extremism propagated by "Jihadi-Salafi" ideology.[18] Rather, this paper will note that extremism results from ideology, not religion, and therefore a broadening definition of extremism is necessary. In this context, this paper will discuss the use of predictive analytics as a tool in identifying, predicting, analyzing, and possibly preventing homegrown extremism propagated from religious, environmental, right wing, left wing, and other persons, located in the United States.

II. NATURE OF THE THREAT AGAINST THE UNITED STATES

Threats against the United States have evolved since World War I. Since that time, the majority involved state actors: Germany[19], Japan[20], Korea[21], and the Soviet Union[22]. However, ever since the Cold War, non-state actors have been the dominant threat to the national security of the United States.[23] These actors have complicated the intelligence and security regimes and thus a reexamination of how we approach national security is required.[24]

However, such a reexamination would not be new for the United States. Acts of individuals not qualifying as states have normally been labeled as crimes either against the law of the state or violations of the law of nations.[25] It was this law enforcement approach to terrorism that led to prosecutions in the 1993 World Trade Center Bombing, the 1994 Manila Air Plot, the 1995 "Blind Sheik" Trial, and the indictment of Osama bin Laden and the Embassy Bombings trials in 1998.[26]

[18] *See* Mitchell D. Silber and Arvin Bhatt, *Radicalization in the West: The Homegrown Threat*, New York City Police Department, at 16-18, (2007).

[19] *American Entry into World War I, 1917*, Office of the Historian, United States Department of State, http://history.state.gov/milestones/1914-1920/WWI.

[20] *Japan, China, the United States and the Road to Pearl Harbor, 1937-41*, Office of the Historian, United States Department of State, http://history.state.gov/milestones/1937-1945/PearlHarbor.

[21] *The Korean War, 1950-53*, Office of the Historian, United States Department of State, http://history.state.gov/milestones/1945-1952/KoreanWar2.

[22] *1945-1952: The Early Cold War*, Office of the Historian, United States Department of State, http://history.state.gov/milestones/1945-1952/foreword.

[23] *See generally* Clapper, James R. Statement to the Senate Select Committee on Intelligence. *Unclassified Statement for the Record on the Worldwide Threat Assessment of the US Intelligence Community*, Hearing, January 31, 2012. Available at: http://www.fas.org/irp/congress/2012_hr/013112clapper.pdf; Accessed April 18, 2013.

[24] *See, e.g.,* John Bellinger, Legal Advisor to the U.S. Sec'y of State, Legal Issues in the War on Terrorism, Address Before the London School of Economics (Oct. 31, 2006), in 8 German L.J. 735, 736 (2007) (raising the question of "whether the existing legal frameworks contained in the Geneva Conventions of 1949 and domestic criminal laws are well-suited to deal with international terrorism in the 21st century."); Anthony Dworkin, Beyond the "War on Terror": Towards a New Transatlantic Framework for Counterterrorism, 13 Eur. Council on Foreign Rel. 1 (2009).

[25] George Terwilliger, Theodore Cooperstein, Shawn Gunnarson, Daniel Blumenthal, and Robert Baker, *The War on Terrorism: Law Enforcement or National Security?*, The Federalist Society for Law and Public Policy Studies, *available at*, http://www.fed-soc.org/publications/detail/the-war-on-terrorism-law-enforcement-or-national-security.

[26] *Fact Sheet: Prosecuting and Detaining Terror Suspects in the U.S. Criminal Justice System*, Office of Public Affairs, United States Department of Justice, (June 9, 2009), *available at*, http://www.justice.gov/opa/pr/2009/June/09-ag-564.html.

However, it was also this reliance on a law enforcement approach to terrorism, the failings of which may have led to the September 11, 2001 attacks on the World Trade Center and Pentagon. However since 2001, the national security establishment has relied on an intelligence-driven approach to combating terrorism, which has not led to successful prosecutions of terrorist suspects.[27]

We are no longer focused on international terrorism. Although, as I argue *infra*, that the security establishment's focus solely on foreign threats for national security purposes is misguided, we are now faced with the threat of a disenfranchised citizen or legal alien becoming radicalized, without foreign influence, on a variety of potential issues, executing a terrorist attack against the United States. As a result, the nature of the response to terrorism needs to combine the two approaches – combining Presidential War Powers and intelligence with local law enforcement mechanisms. This approach is particularly fruitful in the context of identifying, investigating, surveilling, and eventually prosecuting domestic terrorists. This combination of approaches may demand more data collection and analysis capabilities than are currently is use.

A. *Defining a Terrorist and Terrorism*

There is neither an academic nor international legal consensus regarding the definition of the terrorism.[28] However, scholars have identified 109 different definitions of terrorism covering twenty-two different definitional elements.[29] Furthermore, terrorism may be a pejorative.

> "It is a word with intrinsically negative connotations that is generally applied to one's enemies and opponents, or to those with whom one disagrees and would otherwise prefer to ignore… Hence the decision to call someone or label some organization 'terrorist' becomes almost unavoidably subjective, depending largely on whether one sympathizes with or opposes the person/group/cause concerned. If one identifies with the victim of the violence, for example, then the act is terrorism. If, however, one identifies with the perpetrator, the violent act is regarded in a more sympathetic, if not

[27] Serrin Turner & Stephen J. Schulhofer, *The Secrecy Problem in Terrorism Trials*, Brennan Center for Justice, 1, 79-80 (2005).

[28] *See* Myra Williamson, Terrorism, War and International Law: The Legality of the Use of Force against Afghanistan in 2001, p.36-38. Ashgate Publishing (2009), *available at*, http://books.google.com/books?id=ZuJIPP9HfRsC&pg=PA38#v=onepage&q&f=false; Alex P. Schmid, The Routledge Handbook of Terrorism Research, p.39-42. Routledge (2011), *available at*, http://books.google.com/books?id=_PXpFxKRsHgC&printsec=frontcover#v=onepage&q&f=false.

[29] Record, p. 6 (page 12 of the PDF document), citing in footnote 10 Alex P. Schmid, Albert J. Jongman, et al., *Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories, and Literature*, New Brunswick, New Jersey: Transaction Books, 1988, pp. 5-6.

> positive (or, at the worst, an ambivalent) light; and it is not terrorism."[30]

Under U.S. law, terrorism involves "violent acts" or "acts dangerous to human life that are a violation of the criminal laws of the Unites States," occurring either inside or outside the United States, and are intended either to "intimidate or coerce a civilian population," "influence the policies of a government by intimidation or coercion," or "affect the conduct of a government by mass destruction, assassination or kidnapping."[31] Therefore, under U.S. law, terrorism includes actions perpetrated by "Jihadi-Salafi" ideology as well as environmental, animal rights, and right wing and other organizations and individuals.

B. *Fourth Generation Warfare is the Greatest Homegrown Threat to the National Security of the United States.*

Some have identified this new threat against the United States as Fourth Generation Warfare ("4GW").[32] 4GW refers to the loss of nation-state monopoly on combat forces and marks a return to the times of pre-modern conflicts.[33] That is, 4GW includes any war in which one of the major participants is not a state, but rather a violent non-state actor.[34] The elements of a 4GW include, the tactic of terrorism, decentralized structure, attacks on an enemies culture, low intensity conflicts, lack of hierarchy, decentralized planning and financial network, and use of guerilla and insurgency military tactics.[35] Notwithstanding the definition of 4GW, the use of the term aligns closely with insurgency and so these terms will be used hand in hand.[36]

In modern times, 4GW seems to be the dominant threat to nation-states across the globe.[37] 4GW can be traced to the Cold War period when the Soviet-led Afghan forces fought against the mujahedeen in 1979.[38] It has been argued that it

[30] Bruce Hoffman, Inside Terrorism Ch. 1, Columbia University Press 1998, *available at*, http://www.nytimes.com/books/first/h/hoffman-terrorism.html

[31] 18 U.S.C.A. §2331(1), (2) (2001) (defining international and domestic terrorism).)

[32] *See generally* William S. Lind, Col. Keith Nightengale, Capt. John F. Schmitt, Col. Joseph W. Sutton, Lt. Col. Gary I. Wilson, *The Changing Face of War: Into the Fourth Generation*, Marine Corps. Gazette, October 1989, at 12-16, *available at*, http://www.au.af.mil/au/awc/awcgate/milreview/lind.pdf.

[33] *Id.* at 13.

[34] *Id.* Examples may include the American Revolution.

[35] *Id.* at 16.

[36] *See generally* Antulio J. Echevarria II, Fourth-Generation War and Other Myths, Strategic Studies Institute, November 2005, Strategic Studies Institute, *available at*, http://www.strategicstudiesinstitute.army.mil/pdffiles/pub632.pdf.

[37] *See* Clapper, James R. Statement to the Senate Select Committee on Intelligence. *Unclassified Statement for the Record on the Worldwide Threat Assessment of the US Intelligence Community*, Hearing, January 31, 2012. p.3-5. Available at: http://www.fas.org/irp/congress/2012_hr/013112clapper.pdf; Accessed April 18, 2013.

[38] Donald L. Barlett, James B. Steele, *The Oily Americans*, Time Magazine. (May 13, 2003), *available at*, http://www.time.com/time/magazine/article/0,9171,450997-92,00.html.

was after this time; the modern global threat of terrorism began.[39] However such an argument is misguided. In fact, 4GW against the U.S. likely commenced during the civil rights movement with Black Nationalist, Weather Underground, and Left-Wing Militia attacks in the 1970s, which targeted government institutions with explosive and incendiary devices.[40]

In fact, considering all terrorist attacks against the United States from 1970 to 2010, the greatest threat against the national security of the United States is not Islamic extremism, but rather animal rights, environmental, and right wing extremists.[41] As a result, the national focus on "Jihadi-Salafi" ideologically focused extremism as the greatest domestic threat is both dangerous and naive.[42] In fact, from September, 11, 2001 until November 22, 2011,[43] 32.5% of terrorist attacks in the United States were committed by animal rights organizations,[44] 4.5% were committed by anti-abortion rights groups or individuals, and 2.4% were committed by white supremacists.[45] Only 2% of all terrorist attacks since September 11, 2001 involved "Jihadi-Salafi" ideologically focused extremists.[46] Furthermore, the number of Muslim-Americans arrested on terrorism charges as declined steadily from 2009 to 2012.[47] Although such extremists have accounted for a majority of the loss of life in the United States since, and including, the September 11, 2011 attacks,[48] it would be too simplistic to consider Muslim extremists the sole and greatest threat to the United States.

But what does this mean for the national security regime? The US is on the cusp of a changing tide in how homegrown extremism is investigated and tried.[49] The threat is no longer solely from individuals and groups arriving abroad.[50] The

[39] Bergen, Peter, *Holy War Inc.*, p.67, Free Press, (2001),

[40] *See* National Consortium for the Study of Terrorism and Responses to Terrorism (START). (2012). Global Terrorism Database [United States]. Retrieved from http://www.start.umd.edu/gtd/search/Results.aspx?page=21&casualties_type=&casualties_max=&country=217&count=100&expanded=no&charttype=line&chart=overtime&ob=GTDID&od=desc#results-table (Last accessed March 14, 2013).

[41] *See e.g., id.;* Peter Bergen, *Right-Wing Extremist Terrorism as Deadly a Threat as al Qaeda?*, CNN (August 8, 2012), http://www.cnn.com/2012/08/07/opinion/bergen-terrorism-wisconsin.

[42] *See* Mitchell D. Silber and Arvin Bhatt, *Radicalization in the West: The Homegrown Threat*, New York City Police Department, at 16-18, (2007).

[43] The Global Terrorism Database only contains incidents until November 2011.

[44] Animal rights organizations, (ALF, ELF, and others) accounted for 66 terrorist attacks from September 11, 2001 to November 22, 2011. *See supra note 30*.

[45] *Id.*

[46] *Id.*

[47] Charles Kurzman, *Muslim-American Terrorism: Declining Further*, Triangle Center on Terrorism and Homeland Security, p.1, (February 1, 2012), *available at*, http://tcths.sanford.duke.edu/documents/Kurzman_Muslim-American_Terrorism_final2013.pdf.

[48] *See supra note 30*.

[49] John Yoo, *The Terrorist Surveillance Program and the Constitution*, 14 GEO. MASON L. REV. 565, 572 (2006).

[50] *Compare* Mitchell D. Silber and Arvin Bhatt, *Radicalization in the West: The Homegrown Threat*, New York City Police Department, at 16-18, (2007). *with* Charles Kurzman, *Muslim-American Terrorism: Declining Further*, Triangle Center on Terrorism and Homeland Security, p.1, (February 1,

threat includes, and more likely this author argues is greater from, domestic extremists including those espousing religious, political, or radical views with a goal of disrupting the lives of Americans. The domestic threat is planned, managed, and initiated by local residents and citizens.[51] As a result, local law enforcement agencies are on the front lines of interacting with these groups and individuals and the data they collect, in conjunction with open source information, is necessary to ensure the nation is able to protect itself from this growing threat.[52]

Therefore, the traditional national security framework may be inadequate to protect national security and a change is necessary to utilize the benefits predictive analytics could provide the security establishment.

III. THE TRADITIONAL LEGAL AND DATA COLLECTION FRAMEWORK FAILS TO ADDRESS THE THREAT OF HOMEGROWN TERRORISM.

Given the nature of homegrown terrorism, the current legal and data collection framework is insufficient to protect the national security of the United States and must change to allow for domestic intelligence gathering and data analysis and retention.[53]

A. *The Foreign Intelligence Surveillance Act and its Limitations*

The current national security framework encompasses the Foreign Intelligence Surveillance Act (FISA)[54] and the Foreign Intelligence Surveillance Courts (FISCs).[55] Up until 1972, Presidents claimed they had inherent constitutional authority to conduct warrantless electronic surveillance for non-criminal, national security purposes, which was grounded in the Executive's mandate to "preserve, protect, and defend the Constitution of the United States."[56] However, this changed in 1972 when the Supreme Court held, in the *Keith* case, that the Fourth Amendment prohibited warrantless surveillance directed at domestic threats to U.S. national security.[57] In doing so, the Court rejected the government's argument to recognize a foreign intelligence exception to the Fourth Amendment's warrant requirement.[58]

2012), *available at*, http://tcths.sanford.duke.edu/documents/Kurzman_Muslim-American_Terrorism_final2013.pdf.

[51] Mitchell D. Silber and Arvin Bhatt, *Radicalization in the West: The Homegrown Threat*, New York City Police Department, at 5, (2007).

[52] Aziz Z. Huq, Modeling Terrorist Radicalization, 2 Duke F. for L. & Soc. Change, 39, 43 (2010).

[53] *See generally* John Yoo, *The Terrorist Surveillance Program and the Constitution*, 14 GEO. MASON L. REV. 565 (2006)

[54] 50 U.S.C. §1801 *et. seq.* (2010)

[55] 50 U.S.C. §1803 (2010)

[56] U.S. Const. art II, §1. *See* James G. McAdams III, *Foreign Intelligence Surveillance Act (FISA): An Overview*. p.2. Federal Law Enforcement Training Center (FLETC). Located at http://www.fletc.gov/training/programs/legal-division/downloads-articles-and-faqs/research-by-subject/miscellaneous/ForeignIntelligenceSurveillanceAct.pdf, last visited March 18, 2013.

[57] *United States v. United States District Court for the Eastern District of Michigan*, 407 U.S. 297, 315 (1972) (commonly referred to as the *Keith* case).

[58] *Id.* at 340-41.

In response to the Court's decision in *Keith* and the subsequent domestic warrantless surveillance activities during the Nixon Administration, Congress passed FISA in 1978.[59] FISA established three propositions.[60] First, that non-criminal electronic surveillance is permissible to collect foreign intelligence information.[61] Second, foreign powers and foreign agents could be targeted without a warrant.[62] Finally, probable cause must exist before electronic surveillance was permissible.[63] Thus FISA established the only circumstances under which electronic surveillance could be lawfully conducted in the United States for the purpose of collecting foreign intelligence.

The Protect America Act of 2007 amended FISA to allow warrantless surveillance of communications that begin or end in a foreign country without supervision from a FISA Court.[64] In other words, the Act removed the warrant requirement for communications "reasonably believed" to be outside the United States.[65] This Act was confirmed by the FISC.[66]

But what happens when the threat to the United States is not a foreign threat? What if the threat is inspired by the actions of a 'foreign power" or a "foreign agent" but not directed by that entity or agent? What if the threat against the United States is not known or is domestic? Although FISA's "lone wolf" provision may account for such concerns, it only authorizes domestic surveillance of a non-US person who "engages in" or "activities in preparation thereof" *international* terrorism.[67] Furthermore, the FISC judge is required to find that the target had engaged in or was engaging in *international* terrorism.[68]

Judge Richard A. Posner, of the Seventh Circuit, opined that FISA,

> "retains value as a framework for monitoring the communications of *known* terrorists, but it is hopeless as a framework for detecting terrorists. [FISA] requires

[59] McAdams III, James G., *Foreign Intelligence Surveillance Act (FISA): An Overview*. p.2. Federal Law Enforcement Training Center (FLETC). Located at http://www.fletc.gov/training/programs/legal-division/downloads-articles-and-faqs/research-by-subject/miscellaneous/ForeignIntelligenceSurveillanceAct.pdf, last visited March 18, 2013.

[60] 50 U.S.C. §1801 *et. seq.* (2010).

[61] 50 U.S.C. §1802(a)(1)(A)(i) (2010).

[62] 50 U.S.C. §1802(a)(3) (2010).

[63] 50 U.S.C. §1805(a)(2)(A)-(B) (2010).

[64] *See generally* Protect America Act of 2007, Pub.L. 110–55, 121 Stat. 552 (2001).

[65] *See id.*

[66] *See* James Risen, Eric Lichtblau, Eric, *Court Affirms Wiretapping Without Warrants*, New York Times (Jan. 15, 2009), http://www.nytimes.com/2009/01/16/washington/16fisa.html?_r=2&hp&; Evan Perez, *Court Backs U.S. Wiretapping*, Wall Street Journal (Jan. 16, 2009), http://online.wsj.com/article/SB123206893587088395.html?mod=googlenews_wsj; Del Quentin Wilber, R. Jeffrey Smith, *Intelligence Court Releases Ruling in Favor of Warrantless Wiretapping*, The Washington Post (Jan. 16, 2009), http://www.washingtonpost.com/wp-dyn/content/article/2009/01/15/AR2009011502311.html?hpid=topnews.

[67] 50 U.S.C. §1801(b)(1)(C) (2010) (emphasis added).

[68] ELIZABETH B. BAZON, CONG. RESEARCH SERV., RS 22011, INTELLIGENCE REFORM AND TERRORISM PREVENTION ACT OF 2004: "LONE WOLF" AMENDMENT TO THE FOREIGN SURVEILLANCE ACT, 1 (2004).

> that surveillance be conducted pursuant to warrants based on probable cause to believe that the target of surveillance is a terrorist, when the desperate need is to find out who is a terrorist."[69]

Because FISA requires probable cause to investigate threats to national security, it, and the PATRIOT Act assume "the government already has enough information to believe a target is the agent of a foreign power before it even asks for a warrant."[70] But in the domestic context, this may be highly unlikely, and in fact, improbable as seen in Boston. As a result, FISA is inadequate to identify the next domestic threat, let alone unknown foreign threats, to U.S. national security.[71]

B. *Intelligence Reform and Terrorist Prevention Act of 2004 and its Limitations*

The Intelligence Reform and Terrorist Prevention Act of 2004 ("IRTPA") was enacted to revamp the nation's intelligence operations and ease information sharing between investigators pursuing criminal and national security cases.[72] The Act further authorized the creation of "an intelligence center for the purpose of coordinating the collection, analysis, production, and dissemination of open-source intelligence to elements of the intelligence community."[73] This Act benefits the national security regime by facilitating sharing of information in which, as discussed *infra*, individuals do not have a reasonable expectation of privacy.

However the Act falls short in coordinating with state and local law enforcement officials of intelligence relating to the national security of the United States. As discussed earlier, homegrown terrorism often involves violations of traditional crime. Local and State law enforcement has developed community ties and have developed greater expertise in such areas than Federal officials. As a result, the lack of a national-local partnership in sharing information falls short of an effective measure to address homegrown terrorism.

C. *Terrorist Surveillance Program and its Limitations*

In response to the September 11, 2001 terrorist attacks, President Bush created the Terrorist Surveillance Program ("TSP"), which authorized the National Security Agency ("NSA") to intercept communications traveling into and out of the

[69] Richard A. Posner, *A New Surveillance Act*, The Wall Street Journal (Feb. 15, 2006), http://online.wsj.com/article/SB113996743590074183-search.html (emphasis added).

[70] John Yoo, *The Terrorist Surveillance Program and the Constitution*, 14 GEO. MASON L. REV. 565, 573 (2006) (internal citations removed). *See* 50 U.S.C §§1805, 1824 (2010).

[71] John Yoo, *The Terrorist Surveillance Program and the Constitution*, 14 GEO. MASON L. REV. 565, 573-77 (2006).

[72] *See generally* Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638 (2004).

[73] *Id.* at Pub. L. No. 108-458, §1052(a)(1), 118 Stat. 3638 (2004).

United States.[74] According to the program, one of the parties to the communication had to be a suspected member of Al Qaeda.[75]

Although the legality of the TSP has generated much controversy, it has been argued that those opposed to TSP misunderstand constitutional powers.[76] Opponents argue that the TSP amounted to spying on Americans on U.S. soil, in contravention of U.S. wiretapping statutes.[77] However, as former Assistant Attorney General for Legal Policy John Yoo points out, the power to enact the TSP resided in the President's powers in foreign policy, and as commander-in-chief.[78] Because the program focused on foreign threats, the TSP was a lawful exercise of the President's Constitutional authority.

Although the legality of the TSP is of concern for many and a valuable debate, the question critical to this discussion is whether the TSP is an effective mechanism for protecting the nation from homegrown terrorist threats. The TSP allows the federal government to document, intercept, and track electronic communications traveling into and out of the US; however, it is limited to such surveillance if one of the parties is suspected of being a member of Al Qaeda.[79] What if the individual is communicating with someone not known to be associated with Al Qaeda?[80] What if an individual in the US is not communicating with anyone oversees and becomes self radicalized, like the Boston Marathon Bombers?[81]

As a result, the TSP is a program that aids the security establishment by intercepting foreign communications with *known* terrorists, but it of little value to the prevent the threat associated with domestic extremism or unknown threats.[82]

[74] John Yoo, *The Terrorist Surveillance Program and the Constitution*, 14 GEO. MASON L. REV. 565, 565(2006).

[75] See James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, New York Times (Dec. 16, 2005), http://www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=all.

[76] John Yoo, *The Terrorist Surveillance Program and the Constitution*, 14 GEO. MASON L. REV.565, 566(2006).

[77] See Letter from Beth Nolan et al., to the Members of the United States Congress, (Feb. 9, 2006), http://www.nybooks.com/articles/18650; Memorandum from Elizabeth B. Bazan & Jennifer K. Elsea, Congressional Research Service, to various congressional clients (Jan. 5, 2006), *available at* http://www.fas.org/sgp/ crs/intel/m010506.pdf.

[78] John Yoo, *The Terrorist Surveillance Program and the Constitution*, 14 GEO. MASON L. REV. 565, 567-70 (2006).

[79] John Yoo, *The Terrorist Surveillance Program and the Constitution*, 14 GEO. MASON L. REV.. 565, 565(2006).

[80] *See* Richard A. Posner, *A New Surveillance Act*, The Wall Street Journal (Feb. 15, 2006), http://online.wsj.com/article/SB113996743590074183-search.html.

[81] Scott Wilson, Greg Miller & Sari Horwitz, *Boston Bombing Suspect Cites U.S. Wars As Motivation, Officials Say*, The Washington Post (Apr. 23, 2013), http://www.washingtonpost.com/national/boston-bombing-suspect-cites-us-wars-as-motivation-officials-say/2013/04/23/324b9cea-ac29-11e2-b6fd-ba6f5f26d70e_story.html.

[82] *See* Richard A. Posner, *A New Surveillance Act*, The Wall Street Journal (Feb. 15, 2006), http://online.wsj.com/article/SB113996743590074183-search.html.

D. *Lack of Local Law Enforcement in Investigating Terrorism.*

Because domestic extremism may not involve foreign sources or foreign agents, the national security infrastructure has collided with the local law enforcement community in investigating homegrown threats.[83] However, in national security investigations, local law enforcement has largely been ignored from the equation.[84] The NSA's mandate is merely to "collect, process, analyze, produce, and disseminate" intelligence for "foreign intelligence and counterintelligence" purposes.[85] Further, the Central Intelligence Agency ("CIA") has no authority to conduct intelligence investigations in the United States on U.S. persons.[86]

The only Federal agency with domestic national security surveillance and intelligence capability is the Federal Bureau of Investigation ("FBI") through their National Security Branch ("NSB"). This mandate allows the FBI to "conduct counterintelligence and coordinate counterintelligence activities of other agencies within the Intelligence Community."[87] Although Executive Order 12333 provides for collection of information and the techniques to use, such techniques are only coordinated within "[e]lements of the Intelligence Community."[88] Generally, local enforcement are not involved in investigating threats to national security; unless they are part of an FBI Joint Terrorism Task Force ("JTTF"). Although E.O. 12333 authorizes the intelligence community to cooperate with law enforcement, this 'cooperation' does not affirmatively require such coordination and the 'cooperation' may not always result in effective security investigations.[89]

The example in Portland, Oregon is of significance where the Portland Police Chief is the only one granted a security clearance with respect to the JTTF activities.[90] How can the JTTF function appropriately if only one individual is authorized to review the information forming the basis of an investigation? What do we do with all the data that is collected, on the one hand, on a local level, and, on the other, a national level? How do we combine these both with information about global terrorism and terrorism threats that may impact the United States?

The answers to these questions demand local, national, and global cooperation between national security and law enforcement communities, the extended discussion of which is beyond the scope of this paper. Suffice it to say,

[83] See Mitchell D. Silber and Arvin Bhatt, *Radicalization in the West: The Homegrown Threat*, New York City Police Department, at 16-18, (2007).

[84] *See generally* John Yoo, *The Terrorist Surveillance Program and the Constitution*, 14 GEO. MASON L. REV.565, 572 (2006); Mark S. Hamm, *Crimes Committed by Terrorist Groups: Theory, Research and Prevention*, Award No. 2003 DT CX 002, *for* U.S. Department of Justice, (June 1, 2005).

[85] Exec. Order No. 12333 1.12(b), 46 Fed. Reg. 59941 (1981).

[86] *Id.* at 1.8(a), 2.4(a).

[87] *Id.* at 1.14(a).

[88] *Id.* at 2.4 and 2.5.

[89] *See Id.* at 2.6(a).

[90] *See* Bob Heye, *Portland City Counsel Splits on Hotly Debated JTTF Report*, KATU (Mar. 27, 2013), http://www.katu.com/politics/Portland-City-Council-splits-on-hotly-debated-JTTF-report-200362601.html.

even the National Commission on Terrorist Attacks upon the United States ("9/11 Commission") understood that "[c]ounterterrorism investigations in the United States very quickly become matters that involve violations of criminal law and possible law enforcement action."[91] However, within the scope of this discussion, is the necessary collection, analysis, and proliferation of data across state and national lines to ensure appropriate responses to national security and, in particular, homegrown threats.

IV. PREDICTIVE ANALYTICS MAY ENHANCE INTELLIGENCE GATHERING AND THREAT ASSESSMENT AND DETECTION

Predictive analytics has the potential to be an effective tool to identify, track, investigate, and eventually prosecute homegrown extremism. As the current legal infrastructure has developed, the focus has been on foreign influence, agents, or threats and thus law enforcement lacks the tools necessary to identify potential such threats. Predictive analytics and the use of Big Data coupled with a complicated set of algorithms may allow law enforcement to predict the likelihood of extremist behavior based upon past acts, internet posts, current investigations and crimes.

A. *Predictive Analytics Defined*

Predictive analytical solutions "apply sophisticated statistical, data exploitation, and machine-learning techniques to historical information in order to uncover hidden patterns and trends."[92] In other words, predictive analytics is an area of statistical analysis that deals with extracting information from data and using it to predict future trends and behavioral patterns.

As a result, predictive analytics is a "multi-perspective approach that includes integrated reasoning, pattern recognition, and predictive modeling associated with domain knowledge."[93] Therefore, predictive analytics encompasses data mining, predictive modeling, machine learning, and forecasting. Data mining refers to the "practice of using powerful supercomputers and advanced algorithms to analyze vast amounts of information for patterns of behavior."[94] The Government

[91] National Commission on Terrorist Attacks upon the United States. (Philip Zelikow, Executive Director; Bonnie D. Jenkins, Counsel; Ernest R. May, Senior Advisor). *The 9/11 Commission Report*. p.424. New York: W.W. Norton & Company, 2004.

[92] *Leveraging Data for International and External Threat Detection*, IBM, May 2010, at 1, *available at*, http://public.dhe.ibm.com/common/ssi/ecm/en/ytw03044gben/YTW03044GBEN.PDF. Last visited March 19, 2013. The core of predictive analytics relies on capturing relationships between explanatory variables and predicted variables from past occurrences and exploiting them to predict future outcomes.

[93] J Yue, A. Raja, D Liu, X. Wang, and W. Ribarsky, *A Blackboard Approach Towards Predictive Analytics*, 1, Association for the Advancement of Artificial Intelligence (2008) *available at* http://coitweb.uncc.edu/~anraja/PAPERS/TPA_JYue.pdf.

[94] John Yoo, *The Terrorist Surveillance Program and the Constitution*, 14 GEO. MASON L. REV. 565, 577 (2006). For more detailed information on data mining, *see generally* Open Directory Project – Data Mining Database, http://dmoz.org/Computers/Software/Databases/Data_Mining/.

Accountability Office ("GAO") defines data mining as "the application of database technology and techniques – such as statistical analysis and modeling – to uncover hidden patterns and subtle relationships in data and to infer rules that allow for the prediction of future results.[95] Predictive modeling is the process by which a model is created to analyze large data sets and best predict the probability of an outcome.[96] Machine learning is a branch of artificial intelligence that is about the construction and study of systems that can learn from data.[97]

In the national security context, such a regime would operate not to supplant law enforcement investigations, but would serve as an additional tool in the way data is being analyzed and processed in order to flag potential terrorists for future investigation. In the modern Google and Facebook age, "people are the sum of their social relationships, online interactions, and connections with content."[98] Because, as discussed infra, people do not have an expectation of privacy in this content, these relationships can be exploited to enhance our national security.

B. *Technological Challenges*

Predictive analytics is not without its challenges. First, history cannot always predict the future outcome of events. Using historical data to predict future events implicitly assumes that there are steady conditions or constants in a complex system. However, predictive analytics alone is not the answer to domestic national security threats, rather, used in conjunction with traditional law enforcement mechanisms, predictive analytics can be a powerful took in aiding law enforcement to use their resources more efficiently and in identifying and locating potential threats.

Second, in all data collection, there are issues of not knowing the unknowns. The data collector must define the set of variables for which data is collected, which could lead to errors critical to predicting outcomes. However, this is only a problem if were seeking to identify exact future outcomes.[99] Predictive analytics can be used to identify potential threats to national security, which then can be used to help guide law enforcement to the actual, credible, and likely threats. The use of such technology, like traditional investigations, is not a solution to find, with certainty, criminal behavior, but rather to help use resources more efficiently and limit the instances of arbitrary investigations.[100] In fact, in the predictive modeling context, some of the challenges associated with this can be addressed by a property of machine learning called generalization which allows the system to generalize from

[95] U.S. GOVT ACCOUNTABILITY OFFICE, GAO-04-548 , DATA MINING: FEDERAL EFFORTS COVER A WIDER RANGE OF USES (2004).

[96] Mike Batty, et. al., *Predictive Modeling for Life Insurance: Ways Life Insures Can Participate in the Business Analytics Revolution*, Deloitte Consulting LLP, 4, (2010), *available at*, http://www.soa.org/files/pdf/research-pred-mod-life-batty.pdf

[97] *See* Tom M. Mitchell, *The Discipline*, p.1, Carnegie Mellon University (2006).

[98] Viktor Mayer-Schonberger & Kenneth Cukier, *Big* Data, p. 236, Houghton Mifflin Harcourt (2013).

[99] *Id.* at 23.

[100] *See* Colleen McCue, *Connecting the Dots: Data Mining and Predictive Analytics in Law Enforcement and Intelligence Analysis*, Police Chief Magazine, March 2003.

its experiences and learn as more data is included into the process for analyzing.[101] As a result, the national security regime would need to accept the use of "messy" data points to help generate better leads of potential homegrown terrorist suspects.[102]

Finally, the accepted algorithm can be taken advantage of by the developers or users who know how to manipulate the data.[103] This is by far, the biggest and most cumbersome challenge for predictive analytics. How do we ensure that the data is being used in a manner that is legal, efficient, effective, and respectful of our nation's normative values? While such a concern even exists today, with the TSP, such a concern must not shield our eyes from the benefits of predictive analytics, simply because abuse may occur. The development of a predictive analytical regime demands a detailed data collection, access, security and accountability measures.

C. *Private Companies and Government Agencies have Already Been Using Predictive Analytics.*

Private companies have used predictive analytics to predict future risk,[104] consumer behavior,[105] voting behavior,[106] and aid in productivity.[107] Furthermore, even the criminal justice system has developed, in limited contexts, the use of predictive analytics.[108]

In predicting future risk, banks, cell phone providers, internet service providers ("ISP"), insurance companies all use churn models that predict the likelihood that certain customers will switch service providers.[109] These models allow private companies to predict future behavior and allow them to transition

[101] Pedro Domingos, *A Few Things to Know About Machine Learning*, 3, University of Washington.

[102] *See* Viktor Mayer-Schonberger & Kenneth Cukier, *Big* Data, p. 287, Houghton Mifflin Harcourt (2013).

[103] An example of this is when CDO dealers actively fulfilled rating agencies input to reach AAA or super-AAA on the CDO they were issuing by cleverly manipulating variables that were unknown to the rating agencies.

[104] *See generally* Charles Nyce, *Predictive Analytics White Paper*, American Institute for Chartered Property Casualty Underwriters/Insurance Institute of America, p. 1-4 (2007).

[105] *See* Beth Pearsall, *Predictive Policing: The Future of Law Enforcement?*, National Institute of Justice Journal 266, p.1 (June 2010), *available at*, http://www.nij.gov/journals/266/predictive/htm; Colleen McCue, *Connecting the Dots: Data Mining and Predictive Analytics in Law Enforcement and Intelligence Analysis*, Police Chief Magazine, March 2003.

[106] Eric Siegel, *The Real Story Behind Obama's Election Victory*, The Fiscal Times (Jan. 21, 2013) http://www.thefiscaltimes.com/Articles/2013/01/21/The-Real-Story-Behind-Obamas-Election-Victory.aspx#page1.

[107] Viktor Mayer-Schonberger & Kenneth Cukier, *Big* Data, p. 35-37, Houghton Mifflin Harcourt (2013).

[108] *See* Beth Pearsall, *Predictive Policing: The Future of Law Enforcement?*, National Institute of Justice Journal 266, 1, (June 2010), *available at*, http://www.nij.gov/journals/266/predictive/htm; *Police Warm to Predictive Analysis Crime Fighting Tools*, Homeland Security Wire (Sept. 22, 2010), http://www.homelandsecuritynewswire.com/police-warm-predictive-analysis-crime-fighting-tools?page=0,0 (describing the CRUSH program in Memphis Tennessee).

[109] *See* Colleen McCue, *Connecting the Dots: Data Mining and Predictive Analytics in Law Enforcement and Intelligence Analysis*, Police Chief Magazine, March 2003.

their business and marketing strategy to alter future behavior of customers who may be prime to leave their services. Additionally, insurance companies have always relied on forecasting to determine future health risk of their insured.[110]

In the consumer market, Wal-Mart learned, through analytics, that when a major weather threat impacted particular areas, demand for duct tape, bottled water, and strawberry pop-tarts increased.[111] Also, Amazon uses predictive analytics in forecasting what products a consumer is either looking for, will buy, or is potentially interest in, based solely on their searches and buying history.[112] Additionally, Netflix, was able to predict the success of the popular show, *House of Cards*, by knowing how many of their customers were Ken Spacey fans and how many were streaming the British *House of Cards* sitcom.[113] Finally, even Target was able to predict when a female is pregnant or is about to deliver.[114] Target found that a combination of twenty-five products, including unscented lotion, cotton balls, hand sanitizers, and vitamin supplements provided Target with a "pregnancy prediction score."[115] Each of these algorithms allows companies to target particular products to consumers based solely on information the consumer willfully provided the company.

In the voting behavior context, numerous companies have understood that compiling information such as, voting behavior, age, sex, race, home ownership, credit card debt, education, and other factors, they can predict which potential voters would be susceptible to different types of voter outreach programs.[116] For example, in the 2012 election cycle, predictive analytics allowed the Obama Administration to target and influence swing voters.[117] In fact, an Obama "auto-dialer get-out-the-vote programs [decided] who to call and [gave] volunteers a

[110] Charles Nyce, *Predictive Analytics White Paper*, American Institute for Chartered Property Casualty Underwriters/Insurance Institute of America, p. 1 (2007).

[111] Beth Pearsall, *Predictive Policing: The Future of Law Enforcement?*, National Institute of Justice Journal 266, 1, (June 2010), *available at*, http://www.nij.gov/journals/266/predictive/htm.

[112] Ravi Kalakota, *Analytics-as-a-Service: Understanding how Amazon.com is Changing the Rules*, *available a*t, http://practicalanalytics.wordpress.com/2011/08/13/analytics-as-a-service-understanding-how-amazon-com-is-changing-the-rules/.

[113] *See The 'Big Data' Revolution: How Number Crunchers Can predict Our Lives*, National Public Radio, March 7, 2013, *available at*, http://www.npr.org/2013/03/07/173176488/the-big-data-revolution-how-number-crunchers-can-predict-our-lives; Viktor Mayer-Schonberger & Kenneth Cukier, *Big* Data, p. 167, Houghton Mifflin Harcourt (2013).

[114] Kasmir Hill, *How Target Figured Out a Teen girl Was Pregnant Before Her Father Did*, Forbes Magazine (February 16, 2012, http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/.

[115] *Id.*

[116] *Finding Supporters: Political Predictive Analytics Using Logistic Regression*, Multivariate Solutions, *available at,* http://www.mvsolution.com/wp-content/uploads/Predictive-Analytics-for-Finding-Political-Campaign-Supporters.pdf

[117] Robert L. Mitchell, *Election 2012; Obama for America's "Moneyball" Moment*, ComputerWorld (Nov. 6, 2012), http://blogs.computerworld.com/business-intelligenceanalytics/21282/election-2012-obamas-moneyball-moment (characterizing the Obama campaign's use of predictive analytics as the political equivalent as Baseball's 'Moneyball' movement); Mike Gualtieri, *Intro to Predictive Analytics Reading List*, Forrester (Mar. 20, 2013), http://blogs.forrester.com/category/predictive_analytics.

script with a message designed to have the highest probability of moving each micro-targeted segment of voters to action."[118]

In the productivity context, spam filters were designed to automatically adapt the types of email a user receives, filtering 'spam' depending on a combination of who sent the email, the text in the email, and other factors.[119] Furthermore, predictive analytics is used in the "autocorrect feature" in smartphones by tracking user actions and adding new words to its dictionary to increase efficiency and accuracy.[120]

In the criminal justice system, police departments across the United States are using spatial predictive analytics to track crime rates in order to prevent, respond, and use their limited resources more efficiently in order to combat crime.[121] For local law enforcement, the goal is to deploy their resources to areas where the likelihood of future crimes is high; taking into account past crimes, the areas in which the crimes occurred, the demographics of the area and the alleged suspect and many other factors. For example, police in Memphis Tennessee added Criminal Reduction Utilizing Statistical History ("CRUSH") to their arsenal in combatting crime by more than thirty-percent including a fifteen-percent decrease in violent crime over a four-year period.[122] The CRUSH program enables local law enforcement to evaluate incident patterns throughout the city and forecast criminal hot spots to enhance the deployment of law enforcement resources and increase public safety.[123] Additionally, predictive analytics has been used in New York City to predict what factors may be useful in predicting incarceration among felony offenders depending upon a variety of factors such as, prior felony and misdemeanor convictions, marital status, gender, ethnicity, detention status at hearing, days between arraignment and disposition date, conviction charge, and sentence.[124]

Finally, the Department of Homeland Security ("DHS") developed the Future Attribute Security Technology ("FAST") program to help identify potential terrorists by monitoring an individual's pulse rate, skin temperature, breathing, facial

[118] *Id.*

[119] Viktor Mayer-Schonberger & Kenneth Cukier, *Big* Data, p. 20-21, Houghton Mifflin Harcourt (2013)

[120] *Id.*

[121] Pearsall, Beth. Predictive Policing: The Future of Law Enforcement? National Institute of Justice. Located at http://www.nij.gov/journals/266/predictive.htm. Last visited February 5, 2013); Viktor Mayer-Schonberger & Kenneth Cukier, *Big* Data, p. 238-39, Houghton Mifflin Harcourt (2013).

[122] Crime Reduction Utilizing Statistical History (CRUSH) Program, *available at*, http://www.memphispolice.org/blue%20crush.htm; David Hubler, *Predictive Analysis Grows as Crime-Prevention Tool* (Jan. 15, 2013), http//gcn.com/Articles/2013/01/15/Predictive-analysis-crime-prevention-tool.aspx?p=1; Viktor Mayer-Schonberger & Kenneth Cukier, *Big* Data, p. 238-39, Houghton Mifflin Harcourt (2013).

[123] Crime Reduction Utilizing Statistical History (CRUSH) Program, *available at*, http://www.memphispolice.org/blue%20crush.htm; David Hubler, *Predictive Analysis Grows as Crime-Prevention Tool* (Jan. 15, 2013), http//gcn.com/Articles/2013/01/15/Predictive-analysis-crime-prevention-tool.aspx?p=1.

[124] *See generally* Laura Winterfield *Models for Predicting Incarceration – Felony Cases*, Vera Institute of Justice, January 28, 1992.

expression, body movement, pupil dilation, and other physiological patterns.[125] Preliminary tests in September 2008 showed that FAST demonstrated a seventy-eight percent accuracy on mal-intent detection.[126]

D. *Arguments Against the Use of Predictive Analytics in a National Security Context*

Jeff Jonas and Jim Harper, of IBM and the Cato Institute, respectively argue that data mining, a limited idea of what I argue, is not well suited to the terrorist discovery problem because it would waste taxpayer dollars, infringe on privacy and civil rights and misdirect the valuable time of the national security establishment.[127] They argue the national security regime had the information available to avert the September 11, 2001 terrorist attacks, though they failed "to connect the dots."[128] The hijackers had P.O. boxes, email accounts, drivers licenses, bank accounts, ATM cards, used frequent flier numbers, used the same credit cards, and otherwise operated in plain sight.[129] However, this is exactly the reason for implementing predictive analytics into the intelligence regime. Although data mining alone may not be sufficient, adding predictive analytics into the intelligence capabilities and combining it with law enforcement mechanisms, may result in a more efficient domestic national security regime. For example the hijackers may have been automatically identified by the algorithm and triggered for further investigation by local law enforcement rather than waiting for the voluntary sharing and disclosure of information that may have even failed in the most recent terrorist attack in the United States.

Jonas and Harper further argue that the absence of a terrorist profile results in data mining's ineffectiveness in identifying and predicting terrorists.[130] Their argument stems from the fat that there have been a limited number of terrorist attempts, each distinct in terms of planning and execution, showing no "meaningful pattern" indicating planning or preparation.[131] This argument, however, is misguided. The NYPD identified phases of radicalization, which are so broad in their understanding as to be transferable to other threats to national security such as

[125] Viktor Mayer-Schonberger & Kenneth Cukier, *Big* Data, p. 241, Houghton Mifflin Harcourt (2013); Declan McCullagh, *Homeland Security Moves Forward With 'Pre-Crime' Detection*, CNET (Oct. 7, 2011), http://news.cnet.com/8301-31921_3-20117058-281/homeland-security-moves-forward-with-pre-crime-detection/.

[126] Declan McCullagh, *Homeland Security Moves Forward With 'Pre-Crime' Detection*, CNET (Oct. 7, 2011), http://news.cnet.com/8301-31921_3-20117058-281/homeland-security-moves-forward-with-pre-crime-detection/; Alexander Furnas, *Homeland Security's 'Pre-Crime' Screening Will Never Work* (Apr. 17, 2012), http://www.theatlantic.com/technology/archive/2012/04/homeland-securitys-pre-crime-screening-will-never-work/255971/.

[127] Jeff Jonas & Jim Harper, *Effective Counterterrorism and the Limited Role of Predictive Data Mining*, p.1 Policy Analysis No. 584, Dec. 11, 2006.

[128] *Id.* at 2.

[129] *Id.* at 3-4.

[130] *Id.* at 7.

[131] *Id.* at 7-8.

environmental, animal-rights, and right-wing extremism.[132] Furthermore, dismissing the possibility of understanding the general root causes and signatures of domestic extremist activity depending on the type of extremism limits the tool available for security officials. It is precisely because there is no, at the moment, terrorist profile that predictive analytics, and not solely data mining, may prove its worth. Predictive analytics would allow intelligence and law enforcement to develop correlations in the data being retained. Correlation does not imply causation, but that is not the role of intelligence-enforcement in a national security regime. An intelligence driven law enforcement regime, in a predictive analytics framework, would be designed to mine data, develop correlations and rational inferences between seemingly unrelated relevant data points, identify suspects and trigger law enforcement to investigate the potential threats further.

Furthermore, Jonas and Harper decry the cost of predictive data mining as too expensive, overbroad, and a "waste of nationals resources."[133] They note legitimate data capability concerns – such as compiling, relevance, and analysis – which are naturally present given the current technological, structural, and legal framework.[134] Although the cost to implement a predictive analytical framework would likely be substantial, it would likely pay for itself in the long run, making intelligence, and law enforcement mechanisms more efficient much like Richmond, DHS, and Memphis have found before. Furthermore, they are misguided by the differentiating probable cause and reasonable suspicion legal standards from predictive analytics.[135] Both legal standards are dependent on verified facts supported by reasonable inferences to which predictive analytics would add, not supplant. As a result, a potential suspects pattern need not fit into a predictable terrorist or law enforcement pattern, in order for officials to make reasonable inferences on the threat a particular suspect has to U.S. national security.

Finally, is the prospect theory argument that individuals tend to give excessive weight to low probability results when the stakes are particularly high and the outcomes are particularly bad.[136] A subset of this theory is the cognitive heuristics, which are subconscious shortcuts that people use when making critical decisions.[137] However, the concerns these theories implicate are more relevant to the current national security regime. In the intelligence-enforcement regime the predictive analytical framework would not include law enforcement, and their subjective feelings, within the identification process. Officials would be involved in the data accumulation and later investigation, but not in the process of "connecting the dots" to flag potential threats for future investigation. This limits the concerns

[132] Mitchell D. Silber and Arvin Bhatt, *Radicalization in the West: The Homegrown Threat*, New York City Police Department, at 6-7, (2007).

[133] Jeff Jonas & Jim Harper, *Effective Counterterrorism and the Limited Role of Predictive Data Mining*, p. 8-9, Policy Analysis No. 584, Dec. 11, 2006.

[134] *Id.*

[135] *Id.*

[136] Oren Gross, *Chaos and Rule: Should Responses to Violent Crises Always Be Constitutional?*, 112 Yale L.J. 1011, 1040-41 (2003).

[137] *Id.*

of privacy experts that the database would be used to transition services and focuses to non-warranted threats.

E. *Arguments for Predictive Analytics in the National Security Context.*

The use of predictive analytics in the national security context would be designed to accumulate all open-source data and combine it with information received from lawful investigations. The algorithm would then find relationships, associations and suspicious behavior in order to flag persons of interest for future investigation by law enforcement. This encompasses three benefits.

First, predictive analytics adds data to a function law enforcement and national security already engage in - profiling.[138] In other words, the "promise of big data is that we do what we've been doing – profiling – but make it better, less discriminatory, and more individualized."[139] Predictive analytics would allow the intelligence and law enforcement community to use the data they already collect, analyze it, and develop reasonable inferences to help profile potential threats to national security in a more efficient, and potentially more effective, manner. Predictive analytics would allow law enforcement to flag potential threats before the threats are realized and prevent the likelihood of improper profiling, which unnecessarily paralyzes law enforcement investigations.[140]

Second, local law enforcement have used predictive analytics to "reduce the homicide rate by predicting which prison parolees are likely to commit murder and therefore receive more stringent supervision."[141] They have used predictive analytics to predict incarceration among suspects in cases arraigned on felony charges,[142] which crimes are more likely depending on weather patterns,[143]and, comparing which crimes have occurred in the past and analyzing the offenders and victims, and other data, predicting which areas of a city are likely to experience a spike in crime in the future.[144]

Third, domestic extremism and efforts to support it, whether foreign or domestic, "encompass other crimes including fraud, smuggling, money laundering, identify theft and murder" each of which can be investigated and prosecuted with

[138] Viktor Mayer-Schonberger & Kenneth Cukier, *Big* Data, p. 242, Houghton Mifflin Harcourt (2013).
[139] *Id.*
[140] *See* Amy Davidson, *The Saudi Marathon Man*, The New Yorker (April 17, 2013), www.newyorker.com/online/blogs/comment/2013/04/the-saudi-marathon-man.html.
[141] David Huber, *Predictive Analysis Grows as a Crime Prevention-Tool*, GCN (Jan. 15, 2013), http://gcn.com/Articles/2013/01/15/Predictive-analysis-crime-prevention-tool.aspx?p=1.
[142] *See generally* Laura Winterfield *Models for Predicting Incarceration – Felony Cases*, Vera Institute of Justice, January 28, 1992.
[143] Colleen McCue, *Connecting the Dots: Data Mining and Predictive Analytics in Law Enforcement and Intelligence Analysis*, Police Chief Magazine, March 2003.
[144] *See* Beth Pearsall, *Predictive Policing: The Future of Law Enforcement?*, National Institute of Justice Journal 266, p.1 (June 2010), *available at*, http://www.nij.gov/journals/266/predictive/htm; *Police Warm to Predictive Analysis Crime Fighting Tools*, Homeland Security Wire (Sept. 22, 2010), http://www.homelandsecuritynewswire.com/police-warm-predictive-analysis-crime-fighting-tools?page=0,0 (describing the CRUSH program in Memphis Tennessee).

the help of predictive analytics.[145] Domestic and international terrorists do not respect the jurisdictional and national boundaries that exist.[146] In fact, as shown in the case studies below, they often exploit such relationships.[147] Because of this jurisdictional divide, local law enforcement needs to be part of the broader effort to protect the nation from domestic extremism. In connection with this is the promise for more access to data and enhanced data collection methods. The use of predictive analytics would require local and federal authorities, and at some point international authorities, to structure their data collection and retention methods in a manner that allows for broad-based access. This would allow security officials across the nation, and the globe, to benefit from real-time, current, data analysis to enhance their responses to national security threats. The failure of United States to prevent the September 11, 2001 terrorist attacks was not data; rather it was a failure of integration.[148] Provided there is an integrated data accumulation and analysis infrastructure, predictive analytics can accurately model complex interactions, associations, and relationships and use these models to identify and characterize unknown relationships to make reasonable predictions of future events.[149]

The value of predictive analytics is not in its ability, or desire, to supplant traditional intelligence gathering and law enforcement functions. Rather, the value is in using the mass amounts of data the national security infrastructure collects in a manner that makes sense of seemingly diffuse information. How do we know there are no patterns, or there is no terrorist profile if we can't analyze the data? Predictive analytics may offer a solution to some of these problems.

The following cases exemplify the efficacy that predictive analytics could play and the need for local law enforcement involvement, engagement, and leadership in cases of domestic extremism. Although the cases will

i. Ways September 11 could have been identified prior to the attacks.

This paper will not reiterate the findings of the 9/11 Commission.[150] Suffice it to say that the 9/11 Commission noted the failure of the national security establishment to share information and data regarding threats to U.S. national

[145] Colleen McCue, *Datamining and Predictive Analytics: Battlespace Awareness of the War on Terrorism*, Defense Intelligence Journal; 13-1&2 (2005), 47, 48.
[146] *Id.* at 49
[147] *See id.* at 49. *See also infra notes* 150-194 and accompanying text.
[148] National Commission on Terrorist Attacks upon the United States. (Philip Zelikow, Executive Director; Bonnie D. Jenkins, Counsel; Ernest R. May, Senior Advisor). *The 9/11 Commission Report.* p.416-419. New York: W.W. Norton & Company, 2004.
[149] Colleen McCue, *Datamining and Predictive Analytics: Battlespace Awareness of the War on Terrorism*, Defense Intelligence Journal; 13-1&2 (2005), 47, 48.
[150] *See generally* National Commission on Terrorist Attacks upon the United States. (Philip Zelikow, Executive Director; Bonnie D. Jenkins, Counsel; Ernest R. May, Senior Advisor). *The 9/11 Commission Report*. New York: W.W. Norton & Company, 2004.

security was a factor that resulted in the attack.[151] For example, they identified undistributed NSA information that would have helped identify Nawaf al Hazmi.[152] The 9/11 Commission also advised the President to create a "trusted information network" which would serve as a decentralized network model that shares data horizontally, allowing agencies to search within other agencies databases. [153]

Each of the 9/11 Commission's recommendations would enhance national security. However, adding the element of predictive analytics to their substantial recommendations would add even more force to help predict and make reasonable future inferences out of current, messy national security data and information. Predictive analytics would also remove the ego and cultural differences that prevent complete sharing of information. For example, the development of a "trusted information network" combined with a predictive analytics framework and algorithm would allow agencies to not have to 'ask' or 'look' for information themselves. Rather, the algorithm would search across agency jurisdictions to find leads, associations, and connections and alert all intelligence and national law enforcement, and relevant local law enforcement, officials to initiate their own investigations and scrutiny.

ii. Ways Ft. Hood Attack Could Have Been Identified and Prevented.

On November 9, 2009 Major Nidal Malik Hasan, a Medical Corps Officer with the United States Army, engaged in a terrorist rampage in Fort Hood, Texas murdering thirteen and injuring thirty-two active duty service men and women.[154] For a year prior to the attack, the FBI knew of Maj. Hasan's attempts to communicate with known radical extremists and members of al Qaeda.[155] The FBI explained away Maj. Hasan's attempts to communicate with known extremists by saying that he was conducting research.[156]

However, there were other anomalies in Maj. Hasan's background, which may have predicted future criminal behavior. First, before being transferred to Fort Hood in July 2009, Maj. Hasan received a poor performance evaluation.[157] Second, Maj. Hasan conducted a presentation titled "The Koranic World View As It Relates to

[151] National Commission on Terrorist Attacks upon the United States. (Philip Zelikow, Executive Director; Bonnie D. Jenkins, Counsel; Ernest R. May, Senior Advisor). *The 9/11 Commission Report*. p.416-417. New York: W.W. Norton & Company, 2004.

[152] *Id.* at 417.

[153] *Id.* at 418.

[154] James C. McKinley Jr., *Major Held in Fort Hood Rampage is Charged with 13 Counts of Murder*, New York Times (Nov. 12, 2009), http://www.nytimes.com/2009/11/13/us/13inquire.html?_r=0; *Soldier Opens Fire at Ft. Hood; 13 Dead*, CBS News (Nov. 5, 2009), http://www.cbsnews.com/stories/2009/11/05/national/main5539067.shtml.

[155] John Doyle & Chuck Bennett, *FBI Blew Off Killer E-mail to al Qaeda*, New York Post (Nov. 10, 2009), http://www.nypost.com/p/news/national/item_Bqi6bMwstWFXefjamp9CdJ.

[156] *Id.*

[157] *Profile: Major Nidal Malik Hasan*, BBC News (Nov. 12, 2009), http://news.bbc.co.uk/2/hi/8345944.stm; *Gunman Kills 12, Wounds 31 at Fort Hood* (Nov. 5, 2009), http://www.nbcnews.com/id/33678801/ns/us_news-crime_and_courts/t/gunman-kills-wounds-fort-hood/.

Muslims in the U.S. Military" while at Walter Reed Medical Center and suggested that the Department of Defense should allow Muslims the option of being released as 'conscientious objectors' to increase troop morale.[158] Third, in response to the Little Rock, Arkansas murder of two Army recruiters by claimed Al Qaeda terrorist Carlos Bledsoe, a.k.a. Abdulhakim Mujahid Muhammad, Maj. Hasan reportedly made 'outlandish' statements against the US military, suggesting that "Muslims should stand up and fight against the aggressor."[159] Fourth, Maj. Hasan posted on the internet discussing suicide bombings; comparing them to a soldier throwing himself on a grenade to save their colleagues, and noting that suicide bombers sacrifice their life for a "more noble cause."[160] Fifth, ABC News reported that Maj. Hasan had communications with known al Qaeda members beyond simply Anwar al-Awlaki, a U.S. citizen former Virginia imam turned terrorist.[161] Finally, and most importantly, starting in December 2008, Maj. Hasan exchanged as many as twenty email messages with al-Awlaki in 2004. [162] Although these communications may have seemed 'research related,'[163] Maj. Hasan wrote in one email, "I can't wait to join you" in the afterlife.[164] Maj. Hasan's communications with al-Awaki increased in the months before the attack.[165] Al-Awlaki even noted the Maj. Hasan was providing evidence him,[166] leading to an argument that Maj. Hasan could have been investigated and eventually prosecuted for espionage.[167]

[158] Kevin Drum, *Hasan and the "Koranic World View"*, Mother Jones (Nov. 9, 2010), http://www.motherjones.com/kevin-drum/2009/11/hasan-and-koranic-world-view; Dana Priest, *Fort Hood Suspect Warned of threats Within the Ranks*, The Washington Post (Nov. 10, 2009), http://articles.washingtonpost.com/2009-11-10/news/36855074_1_nidal-m-hasan-fort-hood-muslim-soldiers.

[159] Max Fisher, *Why Did Major Hasan Kill 13 at Fort Hood?*, The Atlantic Wire (Nov. 6, 2009), http://www.theatlanticwire.com/politics/2009/11/why-did-major-hasan-kill-13-at-fort-hood/26505/.

[160] Bob Drogin & Faye Fiore, *retracing Steps of Suspected Fort Hood Shooter, Nidal Malik Hasan*, Los Angeles Times (Nov. 7, 2007), http://articles.latimes.com/2009/nov/07/nation/na-fort-hood-hasan7.

[161] Martha Raddatz, Brian Ross, Mary-Rose Abraham, Rehab El-Buri, *Senior Official: More Hasan Ties to People Under Investigation by FBI*, ABC News (Nov. 10, 2009), http://abcnews.go.com/Blotter/official-nidal-hasan-unexplained-connections/story?id=9048590.

[162] Shane, Scott and Dao, James; *Tangle of Clues About Suspect at Fort Hood*, New York Times (Nov. 14, 2009), http://www.nytimes.com/2009/11/15/us/15hasan.html?hp; Martha Raddatz, Brian Ross, Mary-Rose Abraham & Rehad El-Buri, *Senior Official" More Hasan Ties to People Under Investigation*, ABC News (Nov. 10, 2009), http://abcnews.go.com/Blotter/official-nidal-hasan-unexplained-connections/story?id=9048590

[163] Sudarsan Raghavan, *Cleric Says He Was Confidant to Hasan*, The Washington Post (Nov. 16, 2009), http://www.washingtonpost.com/wp-dyn/content/article/2009/11/15/AR2009111503160.html.

[164] Brian Ross & Rhonda Schwartz, *Major Hasan's E-Mail: 'I Can't Wait to Join You' in Afterlife; American Official Says Accused Shooter Asked Radical Cleric When Is Jihad Appropriate?*, ABC News (Nov. 19, 2009), http://abcnews.go.com/Blotter/major-hasans-mail-wait-join-afterlife/story?id=9130339#.UXHq5IJAvdA.

[165] *Id.*

[166] Sudarsan Raghavan, *Cleric Says He Was Confidant to Hasan*, The Washington Post (Nov. 16, 2009), http://www.washingtonpost.com/wp-dyn/content/article/2009/11/15/AR2009111503160.html.

[167] *See* 18 U.S.C §793, *et seq.* (1996).

Although the communications were consistent with "research" Maj. Hasan claimed to have been engaged in, the use of predictive analytics may have allowed officials to develop a more concerted profile of potential threats. Furthermore, the NYPD profile of radicalization, seems to suggest Maj. Hasan engaged in a similar extremist development.[168] Maj. Hasan was reportedly unremarkable, often quietly devout and lived an ordinary lifestyle.[169] Additionally, as a result of visiting the Virginia mosque where al-Awlaki presided in 2001[170] and his growing discontent with the U.S. military and U.S. policy in the Middle East and presentations, Maj. Hasan identified with the Jihadi-Salafi movement.[171] His conversations with known al-Qaida members and al-Qaeda sympathizers further indoctrinated his beliefs, resulting in the attack against US service members.

However, it should not be minimized, nor overly emphasized, that Maj. Hasan suffered a great deal being a Muslim in the U.S. Military. Maj. Hasan was constantly the victim of harassment and anti-Muslim backlash.[172] Similar to other bully incidents,[173] it is not outside the realm of possibility that combining Maj. Hasan's radicalization with his negative experiences in the U.S. Military "pushed him over the edge."

Regardless of this additional motivation, predictive analytics may have allowed the law enforcement and the intelligence community to combine all the pieces and scrutinize Maj. Hasan's actions. Although significant work is still needed to increase coordination among intelligence and law enforcement communities, the inclusion of a national database, the requirement to include a variety of information into the database, and the use of predictive analytics may have provided the FBI with the additional information necessary to prevent the attack.

[168] Mitchell D. Silber and Arvin Bhatt, *Radicalization in the West: The Homegrown Threat*, New York City Police Department, at 6-7 (2007).

[169] James C. McKinley Jr., *Fort Hood Gunman gave Signals Before His Rampage*, The New York Times (Nov. 8, 2010), http://www.nytimes.com/2009/11/09/us/09reconstruct.html; Brett J. Blackledge, *Who is Maj. Nidal Malik Hassan?*, AP (Nov. 5, 2009), http://www.wfaa.com/news/local/69864497.html.

[170] In May 2001, Hassan visited the Dar al-Hijrah Mosque in Fairfax, VA for the funeral of his mother. From January 2001 until 2002, Anwar al-Awaki was the imam of the mosque. *See* Philip Sherwell & Alex Spillius, *Fort Hood Shooting: Texas Killer Linked to September 11 Terrorists*, The Telegraph (UK) (Nov. 7, 2009), http://www.telegraph.co.uk/news/worldnews/northamerica/usa/6521758/Fort-Hood-shooting-Texas-army-killer-linked-to-September-11-terrorists.html.

[171] Brian Ross & Rhonda Schwartz, *Major Hasan's E-Mail: 'I Can't Wait to Join You' in Afterlife; American Official Says Accused Shooter Asked Radical Cleric When Is Jihad Appropriate?*, ABC News (Nov. 19, 2009), http://abcnews.go.com/Blotter/major-hasans-mail-wait-join-afterlife/story?id=9130339#.UXHq5IJAvdA.

[172] Brett J. Blackledge, *Who is Maj. Nidal Malik Hassan?*, AP (Nov. 5, 2009), http://www.wfaa.com/news/local/69864497.html.

[173] *See* Matt Apuzzo & Sharon Cohen, *Va Tech Shooter a "Textbook Killer"*, AP (Sept. 24, 2008), http://www.washingtonpost.com/wp-dyn/content/article/2007/04/19/AR2007041900264_pf.html.

iii. Ways The 'Underwear Bomber" Could Have Been Identified and Prevented.

On Christmas Day 2009, Umar Farouk Abdulmuttalab boarded a flight from Amsterdam to Detroit, Michigan.[174] Abdulmuttalab had boarded with a concealed bomb sewn into his underpants and had attempted to detonate the bomb as the flight approached Detroit.[175] The bomb did not detonate only because after seeing fire, passengers subdued Abdulmuttalab.[176]

However this attack could have been averted through an integrated database and predictive analytics. First, in 2005, while a student at the University College of London Abdulmuttalab was a president of the Islamic Society, an organization who's past presidents have, in the past, been charged with terrorism.[177] During his time at the University, Abdulmuttalab's paths crossed with MI5, U.K.'s domestic counter-intelligence and security agency, for having "multiple communications" with Islamic extremists.[178] Second, Abdulmuttalab had made online postings under the username "farouk1986" on CNN's website saying, among others, "Alight I won't go into too much details about me [sic] fantasy, but basically they are jihad fantisies [sic]. I imagine how the great jihad will take place, how muslims will win insha Allah and rule the whole world, and establish the greatest empire once again!!"[179] Third, despite these security concerns, Abdulmuttalab applied for, and received, a multiple-entry visa to the United States.[180] Fourth, while Abdulmuttalab was in Dubai, he attempted, and failed to gain entry into the U.K. under the auspices of attending a life-coaching program at what British authorities determined to be a fictitious school.[181] Fifth, in November 2009 Abdulmuttallab's father consulted CIA

[174] Indictment in *United States v. Abdulmutallab*, 10-cr-20005, *1, (E.D. Mic. 2010), *available at*, http://www.cbsnews.com/htdocs/pdf/Abdulmutallab_Indictment.pdf

[175] *Id.* at 2.

[176] *Id.*

[177] *Airline Bomb Suspect Reportedly Groomed While a Student in London*, London Times (Dec. 30, 2009), http://www.foxnews.com/story/2009/12/30/airline-bomb-suspect-reportedly-groomed-while-student-in-london/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%253A+foxnews%252Fworld+%2528FOXNews.com+-+World%2529.

[178] *From Shoes to Soft Drinks to Underpants*, The Economist (Dec. 30, 2009), www.economist.com/node/15179544?story_id=15179544&source=hptextfeature; David Leppard, *MI5 Knew of Umar Farouk Abdulmutallab's UK Extremist Ties*, The Sunday Times (London) (Jan. 3, 2010), http://www.timesonline.co.uk/tol/news/uk/article6973954.ece.

[179] Guy Chazan, *Web Offers More Clues on Suspect*, The Wall Street Journal (Dec. 30, 2009), http://online.wsj.com/article/SB126211655382209295.html; Philip Rucker & Julie Tate, *In Online Posts Apparently by Detroit Suspect, Religious Ideals Collide*, The Washington Post (Dec. 29, 2009), http://www.washingtonpost.com/wp-dyn/content/article/2009/12/28/AR2009122802492.html.

[180] *See* Claire Newell, et. al., *Umar Farouk Abdulmutallab: One Boy's Journey to Jihad*, The Sunday Times (London) (Jan. 3, 2010), http://www.timesonline.co.uk/tol/news/world/middle_east/article6974073.ece.

[181] Philip Rucker & Julie Tate, *In Online Posts Apparently by Detroit Suspect, Religious Ideals Collide*, The Washington Post (Dec. 29, 2009), http://www.washingtonpost.com/wp-dyn/content/article/2009/12/28/AR2009122802492.html.

officers in Nigeria and reported of his son's "extreme religious views."[182] Sixth, as a result of these concerns, Abdulmuttalab was placed on the Terrorist Identities Datamart Environment, a database of the U.S. National Counterterrorism Center ("NCTC").[183] At no time was Abdulmuttallab added to the FBI's Terrorist Screening Database, a database feeding the No Fly List and Secondary Screening Selectee List, nor was his multiple-entry visa to the Unites States revoked.[184]

It is clear the U.S. intelligence community failed to prevent a known terrorist from gaining entry into the United States. However, it is possible that a global database relating to the national security of the U.K. and the U.S. and sharing of information between U.S. agencies may have helped further connect the dots to prevent Abdullmuttalab from gaining entry. A predictive analytical intelligence and enforcement regime could have data mined the internet for threatening comments and flagged "farouk1986." It would have identified Abdulmuttallab's travel and denial of U.K. visas as suspicious. The database from which the predictive analytical regime would operate would encompass information from U.K. and U.S. intelligence sources and automatically alert relevant agencies to a possible threat to US national security.

iv. Ways the Times Square Bomber Could Have Been Identified and Prevented.

On May 1, 2010 Faisal Shahzad, a thirty-year-old Pakistani-born naturalized U.S. citizen loaded his Nissan Pathfinder with four different explosive devices and parked it at Times Square.[185] Three difference vendors noticed smoke and fire cracking sounds emanating from the vehicle and alerted the New York City Police Department ("NYPD") who were able to diffuse the bomb and avert a significant domestic terrorist attack.[186] Shahzad was arrested only after he attempted to board a flight from John F. Kennedy International Airport to Dubai.[187] He subsequently admitted to attempting the car bombing, receiving training from a Pakistani terrorist training camp, and was eventually indicted and pled guilty to charges of

[182] Karen DeYoung & Michael Leahy, *Uninvestigated Terrorism Warning About Detroit Suspect Called Not Unusual*, The Washington Post (Dec. 27, 2009), http://www.washingtonpost.com/wp-dyn/content/article/2009/12/27/AR2009122700279.html.

[183] Claire Newell, et. al., *Umar Farouk Abdulmutallab: One Boy's Journey to Jihad*, The Sunday Times (London) (Jan. 3, 2010), http://www.timesonline.co.uk/tol/news/world/middle_east/article6974073.ece.

[184] *Id.*

[185] *Suspicious Car Leads to Closure of Times Square*, CNN (May 2, 2010), http://www.cnn.com/2010/CRIME/05/02/times.square.closure/index.html; *Car Bomb found in New York's Times Square*, BBC News (May 2, 2010), http://news.bbc.co.uk/2/hi/americas/8656651.stm; Peter Grier, *Times Square Bomb: Did Pakistan Taliban Send its 'C' Team?*, Christian Science Monitor (May 10, 2010), http://www.csmonitor.com/USA/2010/0510/Times-Square-bomb-Did-Pakistan-Taliban-send-its-C-team.

[186] William K. Rashbaum, Mark Mazzetti, & Peter Baker, *Arrests in Pakistan Widen Bombing Case*, New York Times (May 4, 2010), http://www.nytimes.com/2010/05/05/nyregion/05bomb.html?hp.

[187] *Id.*

conspiracy to use a weapon of mass destruction and attempting an act of terrorism.[188]

Predictive analytics could have prevented the NYPD from relying on a malfunctioning device,[189] and possibly averted the attack before it occurred or ensured, through an undercover operation, that the components Shahzad used were never going to be effective. First, if there was a fully integrated database of intelligence, officials could have obtained information about Shahzad visiting a Pakistani terrorist training camp through other known terrorist targets and through the help of the Pakistani ISI. Second, Shahzad was listed on a U.S. travel-lookout list since 1999 because he had brought into the US $82,500 in increments of $20,000.[190] Third, intelligence revealed that Shahzad had received a number of phone calls from Pakistan before and after he purchased the Nissan Pathfinder.[191] Second, had the NYPD tracked all license plates driving in and out of Manhattan, like they are planning to do now,[192] they would have noted that the license plate on Shahzad's vehicle was registered to a Ford pick-up truck.

Unfortunately the dots were not connected prior to the attack; however, predictive analytics may have allowed security officials to identify Shahzad before the attack occurred. The investigation revealed a number of anomalies that if put together lead to a reasonable inference of criminal activity. Furthermore, the data points used in the investigation were diffuse, coming from Verizon, JTTF agents, NYPD, Customs and Boarder Protection, and others.[193] Had the data been compiled in a centralized database, law enforcement may have engaged in more active and affirmative investigation of Shahzad and possibly averted the attack.

What each of these case studies show is that from 2001 to today, the national security infrastructure would benefit significantly from predictive analytics. Although in many of the case studies, data sharing was the ultimate culprit in preventing the security establishment from identifying national security threats before the attack, voluntary sharing of information requires individuals to operate against their agencies culture, ego and normal operation – injecting subjectiveness into the analysis. The use of predictive analytics can be a powerful tool, if used

[188] *Times Square Suspect Had Explosives Training, Documents Say*, CNN (May 5, 2010), edition.cnn.com/2010/CRIME/05/04/new.york.car.bomb/index.html; Chad Bray, *Times Square Bomber Gets Life Sentence*, The Wall Street Journal (Oct. 5, 2010) http://online.wsj.com/article/SB10001424052748704469004575533902050370826.html?mod=djemalertNYnews.

[189] Al Baker & William K. Rashbaum, *Police Find Car Bomb in Times Square*, The New York Times (May 1, 2010), http://www.nytimes.com/2010/05/02/nyregion/02timessquare.html.

[190] Yochi J. Dreazan, *Suspect Says He Was Inspired by Imam's Writings*, The Wall Street Journal, (May 6, 2010), http://online.wsj.com/article/SB10001424052748704370704575228150116907566.html?mod=WSJ_latestheadlines.

[191] Complaint in *United States v. Faisal Shahzad*, 6, *available at*, http://s3.amazonaws.com/nytdocs/docs/333/333.pdf.

[192] Cara Buckley, *New York Plans Surveillance Veil for Downtown*, New York Times (July 9, 2007), http://www.nytimes.com/2007/07/09/nyregion/09ring.html?_r=2&.

[193] Complaint in *United States v. Faisal Shahzad*, 7-8, *available at*, http://s3.amazonaws.com/nytdocs/docs/333/333.pdf.

properly, in protecting our national security by removing this subjectivity from the equation and requiring a national database structure.

V. LEGAL FRAMEWORK AND IMPLICATIONS OF THE USE OF PREDICTIVE ANALYTICS AS A DOMESTIC COUNTERTERRORISM TOOL.

The President has the authority, under his power as Commander-in-Chief of the Armed Forces to implement policies relating to national security.[194] However, Congressional support is necessary to appropriate the necessary funds to support such a function.[195] The implementation of predictive analytics can enhance national security and does not run afoul of the Fourth Amendment. It can support a determination of both reasonable suspicion and probable cause. Furthermore, the accumulation and retention of data does not run afoul of the Fourth Amendment.

A. *Authorizations and restrictions*

The President has the authority to implement a predictive analytics regime that combines local and national security apparatuses to repel domestic national security concerns. Presidential authority to engage in intelligence gathering is rooted in the Constitution and relevant case law. The President of the United States, is the "sole organ for the nation in foreign affairs."[196] Under this authority, the President is not stifled by Congress in ratifying treaties,[197] nor in ensuring the national security of the United States. It is under this authority that the President has been authorized to engage in foreign intelligence operations.

Under his authority as "Commander-in-Chief of the Army and Navy of the United States," the President is more than simply a top military commander.[198] Presidential war powers include the "authority to determine when to resort to military hostilities and how to conduct them."[199] This power is enhanced with the President's "executive power" which includes foreign affairs as well as national security.[200] Executive power in the realm of national security is supported by political theorists and ensures the swift, secret, and effective functioning of the security apparatus to protect the United States.[201] It has been this authority that led to the development of the national security infrastructure. This authority allows the

[194] U.S. CONST. art II, § 2, cl. 2.
[195] U.S. CONST. art I, § 12.
[196] *United States v. Curtiss-Wright Export Corp.*, 299 U.S. 304, 320 (1936).
[197] U.S. CONST. art II, § 2, cl. 2.
[198] John Yoo, *The Terrorist Surveillance Program and the Constitution*, 14 GEO. MASON L. REV. 565, 569 (2006).
[199] *Id.* (referencing Alexander Hamilton in The Federalist writing: "Of all the care or concern of government, the direction of war most peculiarly demands those qualities which distinguish the exercise of power by a single hand." The Federalist No. 74, at 500).
[200] U.S. CONST. art II, § 2, cl. 1.
[201] John Yoo, *The Terrorist Surveillance Program and the Constitution*, 14 GEO. MASON L. REV. 565, 570 (2006).

President to engage in defensive operations absent Congressional action or authorization of war.[202]

The Constitution does not vest "Congress any explicit authority to initiate national security policy, nor give[] it an outright veto over executive decisions in the area."[203] However, Congress does possess the power to raise and support armies[204] which has been used to limit Executive power.[205] Congress also has the power to declare war,[206] which, has not been used substantively to prevent the Executive from engaging in defensive security measures.[207] In repelling invasions, the President is the "sole and exclusive judge whether the exigency has arisen."[208]

"While the Constitution diffuses power the better to secure liberty, it also contemplates that practice will integrate the dispersed powers into a workable government. It enjoins upon its branches separateness but interdependence, autonomy but reciprocity."[209] Whether or not there is express or implied authorization by Congress for the President to handle an emergency, the President has inherent authority to protect Americans from domestic terrorist incidents.[210]

It is through this inherent power that the President possesses the authority, within the confines of other protective Constitutional Provisions and Amendments, to order the intelligence community to retain and share information and to develop mechanisms to help predict and prevent domestic terrorist incidents. "The Constitution entrusts the 'power [to] the executive branch of the government to preserve order and insure the public safety in times of emergency, when other branches of the government are unable to function, or their functioning would itself threaten the public safety.'"[211]

Although much of this discussion has related to Presidential War Powers, the crux of this paper surrounds the authority of the Executive to engage in domestic surveillance, within the confines of established limitations, of U.S. citizens, legal

[202] See generally The Prize Cases, 67 U.S. (2 Black) 635 (1863).

[203] John Yoo, *The Terrorist Surveillance Program and the Constitution*, 14 GEO. MASON L. REV. 565, 570 (2006).

[204] U.S. CONST. art I, § 12.

[205] U.S. CONST. art I, § 8, cl. 1. *See* Foreign Assistance Act of 1974 (eliminating all finding for the Vietnam War, effectively ending the Vietnam War); Boland Amendment, Pub. L. 98-473, §8066(a), 98. State. 1937 (1984) (denying further aid to the Contras in Nicaragua); War Powers Resolution, 50 U.S.C. §1541-1548 (1973) (limiting Presidential power to commit the United States to an armed conflict without the consent of Congress).

[206] U.S. CONST. art I ,§ 8, cl. 11.

[207] *See generally The Prize Cases*, 67 U.S. (2 Black) 635, (1863); *In re Neagle*, 135 U.S. 1 (1890).

[208] *Martin v. Mott*, 25 U.S. (12 Wheat.) 19 (1813).

[209] *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 635 (1952).

[210] *The Apollon,* 22 U.S. (9 Wheat.) 362, 366-67 (1824) ([i]t may be fit and proper for the government, in the exercise of the high discretion confided to the executive, for great public purposes, to act on a sudden emergency, or to prevent an irreparable mischief, by summary measures, which are not found in the text of the laws.").

[211] Memorandum Opinion for the Deputy Counsel to the President, The President's Constitutional Authority to Conduct Military Operations Against Terrorists and Nations Supporting Them, September 25, 2001 (quoting *Duncan v. Kahanamoku*, 327 U.S. 304, 335 (1946) (Stone, C.J., concurring)).

aliens, and foreigners for the exclusive purpose of identifying, investigating, preventing, and eventually prosecuting homegrown terrorist threats.

Despite the President's emergency powers, the Constitution ensures that '"[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[212] Therefore, absent an exception, the government cannot engage in a search absent a warrant supported by probable cause.[213]

B. *Predictive Analytics Can Support Reasonable Suspicion And Probable Cause Determinations.*

The Fourth Amendment protects the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable reaches and seizures," unless if conducted pursuant to a warrant supported by probable cause.[214]

There are two issues relating to the intersection of the Fourth Amendment and predictive analytics. First, is whether the use of predictive analytics can support a determination of reasonable suspicion and/or probable cause. Second, whether the data accumulation and retention from police encounters and open source investigations runs afoul of search and seizure law. I argue, in the first, that predictive analytics can be used to support probable cause and reasonable suspicion standards and, in the second, that the retention of information developed by police encounters and open source mechanisms does not run afoul of the Fourth Amendment.

The development of search and seizure law has hinged upon whether an individual has exhibited an expectation of privacy that society is prepared to accept as reasonable.[215] Homes and persons have consistently been given the most protection from warrantless searches due to the invasiveness and intrusiveness of such searches.[216] However, we no longer have a constitutionally-protected expectation of privacy in materials that we voluntarily and knowingly expose to third parties[217] such as where we drive,[218] our license plates,[219] received emails,[220] called phone numbers,[221] or open fields.[222] The voluntary exposure of information

[212] US CONST. amend. IV.

[213] *Id.*

[214] *Id.*

[215] *Katz v. United States*, 387 U.S. 347, 356-57 (1967).

[216] *Bond v. United States*, 529 U.S. 334, 338 (2000); *Kyllo v. United States*, 533 U.S. 27, 40 (2001).

[217] *California v. Greenwood*, 486 U.S. 35, 41 (1988)

[218] *United States v. Knotts*, 460 U.S. 276, 281-82 (1983) ("a person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements…").

[219] *See* Matt Sledge, *NYPD License Plate Readers Will Be Able to Track Every Car Entering Manhattan*, The Huffington Post (Mar. 13, 2013), http://www.huffingtonpost.com/2013/03/13/nypd-license-plate-readers_n_2869627.html.

[220] *Guest v. Leis*, 255 F.3d 325 (6th Cir. 2001).

[221] *Smith v. Maryland*, 442 U.S. 735 (1979). Although the Electronic Privacy Act, 18 U.S.C. §3121 (2001), prohibits the use of pen registers unless consent or a court order is obtained, the Patriot Act allows for the collection of such information.

[222] *Florida v. Riley*, 488 U.S. 445 (1989); *Dow Chemical v. United States*, 476 U.S. 227 (1986).

and the destruction of privacy expectations as a result, have provided the court fodder to continue this analysis in the technology age.

In *Guest v. Leis*,[223] plaintiff's filed a complaint with the Hamilton County, Ohio police department about obscene internet posts.[224] After an investigation, a Hamilton County municipal court judge determined a number of the posts were obscene which formed the basis of a search warrant.[225] In affirming summary judgment for the defendants, the Sixth Circuit held that the website operator's disclaimer that personal communications on the site were not private precluded Fourth Amendment standing and that the users lacked any legitimate expectation of privacy in the internet posts they made on a public site and the emails which were received by a third party.[226]

In *United States v. Perrine*,[227] the Tenth Circuit held that the defendant had no reasonable expectation of privacy in internet subscriber information.[228] Defendant was arrested, charged, and convicted on three counts relating to distribution, receipt, and/or possession of child pornography.[229] As part of the investigation, police had directed Yahoo! to provide subscriber information for the defendant's screen name.[230] In challenging his conviction, defendant argued that he had an expectation of privacy in the internet subscriber information obtained from Yahoo!.[231] The court held, "[e]very federal court to address this issue has held that subscriber information provided to an internet provide is not protected by the Fourth Amendment's privacy expectation."[232]

Both *Leis* and *Perrine* were cases that have come up only post-2000. What about Facebook, MySpace, Twitter? What if a domestic terrorist group uses a combined email account and communicates via unsent drafts rather than sent emails?[233] The popularity of Facebook, Twitter, MySpace, and other social network services as mass communication tools has changed our conception of privacy in the Fourth Amendment context.[234] Insurers, employers, and admissions officers often

[223] 255 F.3d at 329.
[224] *Id.*
[225] *Id.*
[226] *Id.* at 333-34.
[227] 518 F.3d 1196 (10th Cir. 2008).
[228] *Id.* at 1207-08.
[229] *Id.* at 1200.
[230] *Id.* at 1199.
[231] *Id.* at 1204
[232] *Id.* at 1204 (citing *Guest*, 255 F.3d at 336; *United States v. Hambrick*, 225 F.3d 656 (4th Cir. 2000); *United States v. D'Andrea*, 497 F.Supp.2d 117, 120 (D.Mass 2007)
[233] Former CIA Director David Pentreaus used this method to attempt to stay anonymous from Federal authorities as he commenced his love affair with Paula Broadwell. *See* Nicole Perlroth, *Trying to Keep Your E-Mails Secret When the C.I.A. Chief Couldn't*, New York Times (Nov. 16, 2012), http://www.nytimes.com/2012/11/17/technology/trying-to-keep-your-e-mails-secret-when-the-cia-chief-couldnt.html?pagewanted=all.
[234] *See Facebook & Your Privacy: Who Sees the Data You Share on the Biggest Social Network?*, Consumer Reports (June 2012), http://www.consumerreports.org/cro/magazine/2012/06/facebook-your-privacy/index.htm.

mine social networking sites for information to evaluate people.[235] The IRS scans social networking sites to "assist in resolving a taxpayer case."[236] All of this is done under the auspices that a person having no reasonable expectation of privacy in information communicated or stored via such mediums. [237]

As a result, as technology has significantly altered society's expectation of privacy, the *Katz* analysis no longer becomes an impediment to national security investigations, but rather an asset to ensure security officials are not precluded from obtaining information in which a person has no reasonable expectation of privacy.

Furthermore, although warrantless searches, "are *per se* unreasonable," the reasonableness of such a search is subject to a few "specifically established and well-delineated exceptions."[238] Some of these exceptions have been grounded in necessity,[239] administrative compliance,[240] and traditional border and public safety.[241] However, although pen registers statutorily require a warrant,[242] the government need not show probable cause, but rather that its use is "relevant to an ongoing investigation.[243] Furthermore, the in national security context, the PATRIOT Act extended the pen register ability to include addressing information on email, ISP and URL addresses.[244]

The development of the exceptions to the Fourth Amendment warrant requirement allow security officials to obtain a significant amount of information, such as names, addresses, ages, genders, race, information relating to arrests, automobile searches, VIN numbers, phone numbers, banking records, passport information, origination and destination of international travel, and information about past travel. All of this information can be added into a database to enhance the security establishment predict and prevent future domestic terrorist incidents.

Although warrantless domestic surveillance is unconstitutional,[245] "[w]hen the risk is the jeopardy to hundreds of human lives … that danger alone meets the test of reasonableness, so long as the search is conducted in good faith for the

[235] *Id.*
[236] *Id.* (citing a 2009 IRS training manual obtained by the Electronic Frontier Foundation).
[237] Facebook privacy information relating to "public information," *located at*, https://www.facebook.com/about/privacy/your-info.
[238] *Katz v. United States*, 389 U.S. 347, 357 (1967).
[239] *United States v. Robinson*, 414 U.S. 218 (1973) (search incident to arrest); *Michigan v. Long*; 463 U.S. 1032 (1983) (automobile searches); *Michigan v. Tyler*, 436 U.S. 499 (1978) (exigent circumstances); *Terry v. Ohio*, 392 U.S. 1 (1968) (stop and frisk searches).
[240] *Smith v. Maryland*, 425 U.S. 735 (1979) (pen register devices); *United States v. Miller*, 425 U.S. 435 (1976) (banking records); *Skinner v. Railway Labor Executives' Ass'n*, 489 U.S. 602, 628 (1989) (searches to prevent railroad accidents that cause "great human loss"); *Camara v. Municipal Court*, 387 U.S. 523, 539 (1967) (searches to help prevent the spread of disease during a public health crisis).
[241] *United States v. Montoya de Hernandez*, 473 U.S. 532 (1985) (searches person and things entering and leaving the United States); *United States v. Villamont Marquez*, 462 U.S. 579 (1983) (searches of boats on navigable waters); Un*ited States v. Nigro*, 727 F.3d 100 (6th Cir. 1984) (searches of airplanes).
[242] 18 U.S.C. §§3121-3127 (2006).
[243] *Id.* at 3123(a).
[244] USA Patriot Act of 2001, Pub. L. No. 107-56, §216, 115 Stat. 272, 288-290 (2001)
[245] *United States v. United States District*, 407 U.S. 297, 323 (1972).

purpose of preventing hijacking or like damage and with reasonable scope, and the passenger has been given notice of his liability to such a search so that he can avoid it by choosing not to travel by air."[246]

However, the Court may, in the future find a more delineated national security exception in the context where, if the danger is so great, there need not be a showing of reliability of the information supporting a warrantless search.[247] Although this paper will not discuss the efficacy of such an exception, I note that although such an exception would pose privacy concerns, it would allow security officials an additional tool to enhance national security. Furthermore, the proclivity of the Court to not require an "indicia of reliability" of information to support the warrant exception may lead to the Court's acceptance, support or tacit approval of, the use of predictive analytics as an intelligence and investigatory tool.[248]

Even if there is an expectation of privacy that society is prepared to accept as reasonable, security officials can obtain information if they possess reasonable suspicion to stop,[249] or probable cause to search or arrest, with or without a warrant.[250]

i. Predictive Analytics Can Help Develop Reasonable Suspicion.

In the reasonable suspicion scenario, police may briefly detain a person if the person has been, or is about to, engage in criminal activity.[251] Police officers often engage in brief, non-custodial traffic stops supported by reasonable suspicion, when the officer weighs the totality of the circumstances to determine whether the individual engaged in criminal activity.[252] Finally, even without reasonable suspicion, U.S. Customs officials often engage in routine suspicionless searches of people and effects crossing the border without reasonable suspicion.[253] However, where reasonable suspicion is required, there must be more than an "inchoate and unparticularized suspicion."[254] The suspicion must be based on "specific and articulable facts" "taken together with rational inferences from those facts."[255]

[246] *United States v. Edwards*, 498 F.2d 496, 500 (2d. Cir. 1974).

[247] *Florida v. J.L.*, 529 U.S. 266, 273-74 (2000)("We do not say, for example, that a report of a person carrying a bomb need bear the indicia of reliability we demand for a report of a person carrying a firearm before the police can constitutionally conduct a frisk.").

[248] *See* Viktor Mayer-Schonberger & Kenneth Cukier, *Big* Data, p. 287, Houghton Mifflin Harcourt (2013) ("…in some cases big and messy can even be beneficial, since when we tried to use just small, exact portion of the data, we ended up failingto capture the breadth of detail where so much knowledge lies.").

[249] *New Jersey v. T.L.O*, 469 U.S. 325, 346-47 (1985) ("But the requirement of reasonable suspicion is not a requirement of absolute certainty: sufficient, not certainty is the touchstone of reasonableness sunder the Fourth Amendment…") (internal citations removed); *Terry v. Ohio*, 392 U.S. 1, 30 (1968) (holding as constitutional, so-called Terry stops).

[250] US Const. amend IV.

[251] *Terry v. Ohio*, 392 U.S. 1, 33 (1968).

[252] *United States v. Arvizu*, 534 U.S. 266 (2002). *See Terry*, 392 U.S. at 30.

[253] *United States v. Montoya de Hernandez*, 473 U.S. 532 (1985).

[254] *Terry*, 392 U.S. at 27.

[255] *Id.* at 21.

The data, information, and reasonable inferences developed by predictive analytics, would also support a reasonable suspicion determination. Officers often rely on their training and experience in reviewing factual scenarios to determine if there is an articulable suspicion of criminal activity.[256] The same is involved with predictive analytics. The predictive analytical algorithm would use the data to make reasonable and rational inferences based on specific and articulable facts and data to support a reasonable suspicion standard. In fact this is how predictive analytics is currently being used. Target uses predictive analytics to make rational inferences to ensure their shelves are stocked with supplies if a given weather pattern arrives in a particular area.[257] Smartphones use these algorithms to learn more words and analyze user style to make reasonable inferences about what a user meant when they mistyped a message.[258] Local police use this idea to make reasonable and rational inferences from past crimes and information to predict the locations of future crimes to better manage their limited resources.[259] Therefore, predictive analytics is not a foreign concept in the reasonable suspicion context. The algorithm itself can use "specific and articulable facts" to make "rational inferences from those facts."[260]

ii. Predictive Analytics Can Help Develop Probable Cause.

In the probable cause scenario, probable cause "deal[s] with probabilities."[261] In *Brinegar v. United States*,[262] officers observed the defendant driving a vehicle, and relied on their previous encounters with the same to lead to a probability that the defendant was engaged in the illegal importation of alcohol and thus support a probable cause determination.[263] In *Illinois v. Gates*,[264] police were anonymously tipped to the activities of drug traffickers.[265] Police engaged in surveillance and confirmed the information in the tip to support a warrant application.[266] The Court rejected the lower court's assertion of a lack of probable cause based on the lack of the tips reliability on account that based on the totality of the circumstances, the officers had a practical nontechnical conception and particularized suspicion based

[256] *Terry*, 392 U.S. at 21.

[257] Beth Pearsall, *Predictive Policing: The Future of Law Enforcement?*, National Institute of Justice Journal 266, p.1 (June 2010), *available at*, http://www.nij.gov/journals/266/predictive/htm.

[258] Viktor Mayer-Schonberger & Kenneth Cukier, *Big* Data, p. 21, Houghton Mifflin Harcourt (2013).

[259] *See* Crime Reduction Utilizing Statistical History (CRUSH) Program, *available at*, http://www.memphispolice.org/blue%20crush.htm; Colleen McCue, *Connecting the Dots: Data Mining and Predictive Analytics in Law Enforcement and Intelligence Analysis*, Police Chief Magazine, March 2003; *Police Warm to Predictive Analysis Crime Fighting Tools*, Homeland Security Wire (Sept. 22, 2010), http://www.homelandsecuritynewswire.com/police-warm-predictive-analysis-crime-fighting-tools?page=0,0 (describing the CRUSH program in Memphis Tennessee).

[260] *Terry*, 392 U.S. at 21.

[261] *Brinegar v. United States*, 338 U.S. 160, 175 (1949); *Maryland v. Pringl*e, 540 U.S. 366, 370 (2003).

[262] 338 U.S. 160 (1949)

[263] *Brinegar*, 338 U.S. at 169.

[264] *Illinois v. Gates*, 462 U.S. 213 (1983).

[265] *Id.* at 217.

[266] *Id.* at 226.

on the letter, documentation of explicit conduct, and the officer's independent investigation, that a crime was occurring.[267] As a result probable cause denotes a "fair probability" of criminal activity based on a totality of the circumstances.[268]

In both of the aforementioned cases, data from previous encounters and, arguably, imprecise information combined with a current investigation resulted in a finding of probable cause. In a predictive analytical regime, the use of algorithms can allow security officials to argue "fair probability" based on a variety of data points that lead to a probability of criminal activity. In fact, the data points that would be relied upon would arguably be more reliable than the information relied upon in *Brinegar* because it would be based upon both subjective and objective sources, as opposed to the purely subjective feelings of officers.[269] Therefore, substituting data mining and predictive analytics for the tip's specificity in conjunction with the investigator's independent investigation would likely lead to a court finding of probable cause, *before* the threat is realized. In *Gates*, the police relied upon an informant's tip of criminal activity; however, in a national security or lone wolf scenario, security officials may not be so fortunate. They may only know about a person's associations, phone calls, banking records, travel information, and suspicious purchases; however, all of this information could result in a probable cause determination.

iii. Legal Analysis of Both Reasonable Suspicion and Probable Cause Support the Use of Predictive Analytics.

Both reasonable suspicion and probable cause can be supported by the use of predictive analytics. A predictive analytical regime would combine data mining of open-source information, information learned through searches developed by reasonable suspicion and probable cause, and an officer's independent investigation to intercept domestic terrorist plots.

However, in the traditional reasonable suspicion and probable cause analysis there is a reliance on the reliability of the method of the determination and the data being used to support such a determination. In the past, the reliability has been focused on past investigations and police conduct. While the reliability of the process is, admittedly, a concern, it is only one of knowledge and development as opposed to inherence. In other words, as technology progresses, the law must progress as well, learning how these additional tools can be used, how they can be made more effective, how they collaborate within the existing legal structure, and how the existing legal structure may need to be altered to allow for new technological developments. The use of unreliable sources is not new for the courts and the judiciary in determining reasonable suspicion or probable cause.

The Supreme Court, in *Adams v. Williams*,[270] allowed police to rely on an informant's tip to support a reasonable suspicion determination. In *Adams*, the

[267] *Id.* at 231. *See also Brinegar*, 338 U.S. at 176.
[268] *Brinegar*, 338 U.S. at 176.
[269] *Brinegar*, 338 U.S. at 162-164.
[270] *Adams v. Williams*, 407 U.S. 143 (1972).

officer, alone and in a high crime area was confronted by an informant who identified the defendant as being in possession of a gun and drugs.[271] The officer went to the indicated house, and upon seeing the defendant immediately grabbed the waistband of the defendant, despite not himself actually seeing the presence of a weapon.[272] In addition to relying upon the officer's previous experiences with the informant, the Court emphasized that the information carried enough reliability to justify the forcible search.[273]

The holding of *Adams*, that stop and frisks and reasonable suspicion can be supported by information from third parties, is highly relevant and analogous to the use of predictive analytics. Predictive analytics uses articulable facts from a variety of sources – in particular law enforcement and security officials – to support reasonable inferences of future behavior. In fact, the use of the "messy" data in predictive analytics would in fact be *more reliable* than the information upon which the officer relied upon in *Adams*. The information would be provided by a variety of security officials, which would inherently contain corroboration problems, which the algorithm would solve by continually analyzing and comparing the data to already added information. Any determinations or "red flags" would be developed by analyzing all the data points relating to a particular action or individual – including those that would clear a suspect. These 'red flags' would then trigger law enforcement officials to further investigate in order to corroborate, or discount, potential leads. As a result, the predictive analytics regime, consistent with the argument in this article, would not replace traditional investigations or intelligence, but rather help stream line intelligence and investigations in a manner that identifies areas of law enforcement investigation that will likely be fruitful.

In a domestically analogous situation, predictive analytics would not be the constitutional equivalent of the device in *United States v. Kyllo*.[274] In *Kyllo*, officers, suspecting the defendant was growing marijuana, used a thermal imaging device to measure the energy and heat emanating from defendant's home and compared it to other homes.[275] The police argued that the information generated from the device, combined with informant tips and utility bills, supported a search warrant.[276] In finding the practice unconstitutional because no probable cause existed, Justice Scalia emphasized the sacred nature of the home.[277] However, predictive analytics would not invade the home, nor the person. It would simply compile information from a variety of sources in order to track potential criminal behavior.

Another argument against the use of predictive analytics for reasonable suspicion and probable cause determinations is the idea that there has not been a database developed of all terrorist incidents and the development of a "terrorist paradigm" to which the database can be compared. In other words, the retention of

[271] *Id.* at 144-45.
[272] *Id.* at 145.
[273] *Id.* at 147.
[274] 533 U.S. 27, 40 (2001).
[275] *Id.* at 29-30.
[276] *Id.* at 30.
[277] *Id.* at 33.

data is irrelevant if it cannot compare such data to a paradigm that suggests with a reasonable degree of certainty, terrorist activity.

Again, this is not a problem of inherence, rather one of knowledge and development. For example, the NYPD has developed, based upon an admittedly limited number of incidents, the radicalization process of Muslims in the West.[278] This analysis has been furthered in the federal context for white supremacists, Muslims, Blacks.[279] The fact that a terrorist profile has not been developed does not preclude a predictive analytical regime from working. In fact, the reliance on a "profile" may be counterproductive in national security and lone wolf scenarios because not finding a particular individual "fitting neatly" in the box and moving on to a different lead may result in national security problems.[280] National security investigations should encompass a variety of data points to ensure over inclusiveness as opposed to under inclusiveness.

The use of predictive analytics would be akin to the device in *United States v. Karo*.[281] In *Karo*, the Drug Enforcement Agency (DEA) learned that Karo had purchased fifty gallons of ether and suspected Karo was using the substance to remove cocaine from clothing in a large-scale narcotics operation.[282] The DEA then placed a location beeper in the ether barrel, with the owners consent, to monitor the barrel to reveal the location of Karo's drug operation.[283] In holding that the placement of the beeper was not a search, the court relied on the fact that the beeper infringed no privacy interest since it was turned on and off and did not constantly monitor Karo's activities.[284] Furthermore, although the Court held the monitoring of the beeper implicated the Fourth Amendment, this was only the case because monitoring of the beeper "reveal[ed] a critical fact about the interior of the premises that the Government was extremely interested in knowing and that it could not have otherwise obtained without a warrant."[285] Justice White noted the differences between *Karo* and *Knotts*; identifying that a home demands greater protection.[286]

In the case of a predictive analytical algorithm, application of the technology would implicate similar issues as in *Karo*. It would not be used constantly to track the behavior of a person who has a privacy interest in such issues, rather it would effectively be 'turned on and off' at particular times to track behavior such as suspicious buying patterns, foreign travel, and suspicious public internet postings. Further, the tracking the algorithm would engage in would not involve aspects that

[278] Mitchell D. Silber and Arvin Bhatt, *Radicalization in the West: The Homegrown Threat*, New York City Police Department, at 6-10, (2007).
[279] Colleen McCue, *Connecting the Dots: Data Mining and Predictive Analytics in Law Enforcement and Intelligence Analysis*, Police Chief Magazine, March 2003.
[280] *See supra* note 240 and accompanying text.
[281] 468 U.S. 705 (1984).
[282] *Id.* at 708.
[283] *Id.* at 708-09.
[284] *Id.* at 711.
[285] *Id.* at 715 .
[286] *Id.*

would invade the home, the person, or effects.[287] It would track public information and combine it with law enforcement- or intelligence-generated information to help track and make future predictions of future behavior. As a result, the use of predictive analytics would not be alien to the current legal regime.

Finally, the predictive analytical regime is be analogous, to the recent Supreme Court case, *United States v. Jones,*[288] though *Jones* would not preclude the use of the system. In *Jones*, an FBI-MPD joint investigation of defendant's narcotics activities led to the installation of a GPS device on the undercarriage of defendant's vehicle while it was parked in a public parking lot.[289] Investigator's tracked defendant's vehicle twenty-four hours a day for twenty-eight days and documented over two-thousand pages of information relating to defendant's criminal activity based on which he was convicted.[290] In overturning the conviction, the Supreme Court narrowly held the installation of the GPS device constituted a search and thus violated the Fourth Amendment if done without a warrant.[291] Although four of five justices were inclined to find the continual tracking a violation of defendant's reasonable expectation of privacy, the majority did not address whether the warrantless tracking on public streets violated the Fourth amendment.[292] Justices Alito and Sotomayor concurred in judgment and found the continual tracking to be a violation of defendant's reasonable expectation of privacy.[293] However, as noted by the majority, "the *Katz* reasonable-expectation-of-privacy test has been *added to,* not *substituted for,* the common-law trespassory test."[294] Therefore, a trespass may still be a necessary condition to finding, as the majority did in *Jones*, a Fourth Amendment violation.[295] The Court's decision in *Jones* has three implications for predictive analytics.

First, predictive analytics is not analogous to the installation of the GPS device in *Jones* because there is no trespass involved in data mining for open source software or retention of such data for analyzing. Such processes would simply mine the Internet and surveillance video for information that individuals reveal to third parties – implicating neither trespassory nor privacy interests.

Second, if predictive analytics is seen as analogous to the four Justices' finding continual tracking in *Jones*, it is likely the practice would be still be upheld unless there is a change in the make up of the Justices. As noted by Justice Scalia, *Katz* simply added the reasonable expectation of privacy analysis to the trespass regime inherent in Fourth Amendment jurisprudence.[296] Under this analysis, data mining open source information on the internet and compiling such information would not violate the Fourth Amendment.

[287] *See* US CONST. amend. IV.
[288] 132 S.Ct 945 (2012).
[289] *Id.* at 948.
[290] *Id.* at 948-49.
[291] *Id.* at 953.
[292] *Id.* at 954-56 (Sotomayor, J., concurring).
[293] *Id.* at 964 (Alito, J., concurrence). *See id.* at 955 (Sotomayor, J., concurrence).
[294] *Id.* at 952 (emphasis in original).
[295] *See id.* at 952-955.
[296] *Id.* at 952 (emphasis in original).

Third, and more likely, predictive analytics is not analogous to the continual tracking of a suspect with the detail of a GPS device. GPS devices can track entire driving patterns, locations within curtilage of property, and identify locations for quick apprehension. Predictive analytics on the other hand, would only provide information about suspicious purchases, facial recognition in major cities, tracking of a vehicle entering and exiting major cities, and data mine open source information. The system, in effect would turn on and off periodically similar to the device in *Karo*. As a result, the predictive analytical regime would not run afoul of the Fourth Amendment nor Supreme Court precedent.

As a result, in the predictive analytical age, the continual, physical, electronic data retention, and in limited cases surveillance, of individuals by a computer would not violate the Fourth Amendment unless there is a change in the Supreme Court make-up. In fact, even if there is a change, the Supreme Court would have to overrule decades of Fourth Amendment jurisprudence in order to hold that continual electronic surveillance of activities that individuals engage in public thoroughfares, implicating no trespassory interests, demand protection of the Fourth Amendment.[297]

Given this change in technology and the reliance of some Justices on finding a reasonable expectation of privacy in information we voluntarily expose to third parties the question remains whether a database and algorithm that compiles this information without affirmative law enforcement action, or if the implementation of the algorithm in a national security context would run afoul of the Fourth Amendment. In the latter, the Supreme Court has often deferred to the judgment of the Executive in relation to security matters.[298]

In the end, predictive analytics can support reasonable suspicion and probable cause determinations to help security officials predict, investigate, prevent, and prosecute homegrown terrorists. In *Gates*, the police relied upon an informant's tip of criminal activity; however, in a national security or lone wolf scenario, security officials may not be so fortunate.[299] They may only know about a person's associations, phone calls, banking records, travel information, and suspicious purchases; however, all of this information, combined with traditional law enforcement investigations, could result in a probable cause determination prior to an attack rather than after.

For example, Improved Explosive Devices ("IEDs") can be made by a variety of household and common products.[300] Through the Bomb-Making Materials

[297] *See id.*

[298] *See* Cass R. Sunstein, *Administrative Law Goes to War*, 118 HARV. L. REV. 2663, 2672 (2005) ("In war no less than in peace, the inquiry into presidential authority can be organized and disciplined if it is undertaken with close reference to stand principles of administrative law."); Eric A. Posner & Cass R. Sunstein, *Chevronizing Relations Law*, 116 Yale L.J. 1170, 1199 (2007) (calling for deference when "there is no interpretation of a statutory term but simply a policy judgment by the executive").

[299] *See* Jeff Black, *Timeline: Tragedy at the Boston Marathon*, (April 15, 2013), http://usnews.nbcnews.com/_news/2013/04/15/17767941-timeline-tragedy-at-the-boston-marathon?lite.

[300] The Department of Homeland Security, Bomb Making Materials Awareness Program, *available at*, http://www.dhs.gov/bomb-making-materials-awareness-program.

Awareness Program ("BMAP"), DHS seeks to expand awareness and collaboration with federal and local law enforcement agencies as well as local businesses to reinforce community safety.[301] But what if a potential terrorist buys these products from multiple businesses to lower the risk of raising suspicions among a single vigilant business owner? What if information about buying habits and the name, and credit card information, are placed in a national database? What if the database includes other information about names, travel information, other buying habits, of potential targets? Combine all this information with an algorithm that filters through and identifies, based on probabilities, the risk factor of a particular individual to engage in criminal or domestic terrorist activity. In this case, and many more like it, law enforcement can more quickly identify and investigate homegrown threats.

This is the true value of predictive analytics in the national security context as related to probable cause and reasonable suspicion. Instead of simply waiting for an undercover agent to infiltrate a group or association – which may require a sympathetic informant – security officials would be able to identify a potential domestic threat much earlier than before. In the end, predictive analytics does not alter the reasonable suspicion and probable cause analysis. In fact, it supplements the activities of law enforcement by providing them additional information regarding potential suspects, and limits the opportunity of subjective feelings tainting an investigatory process.

C. *The Accumulation and Retention of Information Developed by Police Encounters, Investigations and Open Source Mechanisms Does Not Run Afoul of the Constitution*

Until 1989, when the Berlin Wall fell, East German state security agency, known as the Stasi, spied on millions of people resulting in over 39 million index cards and 70 miles of documents recording and detailing the most intimate aspects of people's lives.[302] This is the fear many people have with using predictive analytics in the criminal justice and national security context. The idea stems from the Hollywood blockbuster *Minority Report* in which Tom Cruise, a pre-crime agent, arrests and detains individuals based solely on what the individual *might* do, rather than what they *did* do. These concerns also encompass the transformation of society into Orwell's 1984;[303] in other word, the threat of predicting future behavior through past behavior and the resulting surveillance state that would result.[304]

However such concerns may be overstated. Companies currently use these methods for marketing and advertising campaigns as well as weighing risk.[305] The real threat of the perpetual surveillance state is that the surveillance alone would

[301] *Illinois v. Gates*, 462 U.S. 213 217 (1983).

[302] Viktor Mayer-Schonberger & Kenneth Cukier, *Big* Data, p. 226, Houghton Mifflin Harcourt (2013)

[303] Viktor Mayer-Schonberger & Kenneth Cukier, *Big* Data, p. 227, 229, 377-78, Houghton Mifflin Harcourt (2013)

[304] *Id.* at 227.

[305] *Id.*;

result in chilling our freedoms and constrain liberty.[306] As the argument goes, predictive analytics would allow the police, to arrest and detain a person based solely on the probability that he or she is going to engage in criminal activity, which negates our historical focus on the presumption of innocence.[307]

However, such concerns are more to do with the structure and implementation of predictive analytics into the criminal justice and national security infrastructure, than with the idea alone. The concerns originate from the detention of individuals before a crime occurs. However, in the national security context this occurs all the time.[308] In each of these situations, government officials intervened in a plot against the United States as he plot was being developed. Most reasonable people would agree that such actions are *exactly* what we expect from our government.

This is the value of predictive analytics. The regime would employ an algorithm to data mine open source and criminal justice information to flag individuals that have a reasonable likelihood of engaging in terrorist activity in the United States. The responsibility then would be on law enforcement to investigate and gather evidence in support, or negation, of this presumption of criminality. The use of open-source data to justify liberty restrictions would not be allowed, rather, as in the context of traditional law enforcement investigations, the algorithm would replace the reliance on informants, tips, or chance encounters used to initiate criminal investigations today, which even now are not necessarily enough to justify detention or restrictions on liberty.

Assuming predictive analytics can support a government finding of reasonable suspicion and probable cause, as the government collects information relating to national security, the accumulation and retention of such data does not violate the Fourth Amendment.

i. Current Review of Collection Methods.

It is first important to understand how the government collects information relating to domestic national security initiatives. Corporations retain massive amounts of data on customers ranging from their personal information through membership and credit cards to their buying and spending habits in order to facilitate marketing and advertising initiatives.[309] If the company is based in the

[306] *Id.* at 241.

[307] Viktor Mayer-Schonberger & Kenneth Cukier, *Big* Data, p. 244, Houghton Mifflin Harcourt (2013).

[308] Chelsea Carter, *Congressman: Thwarted Terror Plot Targeted Train from Canada to U.S.*, CNN (Apr.22, 2013), http://www.cnn.com/2013/04/22/world/americas/canada-terror-plot-thwarted/index.html; Vikram Dodd, *Three Jailed Fir Discussing Possible Terror Attack*, The Guardian (UK) (Apr.25, 2013), http://www.guardian.co.uk/uk/2013/apr/25/three-jailed-possible-terror-attack.

[309] *See* Beth Pearsall, *Predictive Policing: The Future of Law Enforcement?*, National Institute of Justice Journal 266, p.1 (June 2010), *available at*, http://www.nij.gov/journals/266/predictive/htm; Colleen McCue, *Connecting the Dots: Data Mining and Predictive Analytics in Law Enforcement and Intelligence Analysis*, Police Chief Magazine, March 2003. Viktor Mayer-Schonberger & Kenneth Cukier, *Big* Data, p. 88, Houghton Mifflin Harcourt (2013).

United States, the FBI can obtain access to transactional and other data by means of a National Security Letter ("NSL").[310] A NSL is a demand letter that is used by the FBI when investigating matters relating to national security and is limited to non-content information such as transactional records, phone numbers dialed, or e-mail addresses mailed to and from.[311] Although NSLs also include a gag order preventing the recipient of the letter from disclosing that the letter was ever issued, such orders have been found unconstitutional in *Doe v. Gonzalez*[312] and *In re National Security Letter*[313] though the Supreme Court has yet to opine on the matter. Despite these rulings, the use of NSLs is likely to continue.

The FBI also uses the Digital Collection System Network ("DCSNet") to access cellphone, landline, and SMS communications anywhere in the United States.[314] This system allows the FBI, after being issued a warrant, to monitor the network themselves as opposed to waiting for the telecommunications firm to create the tap itself.[315] The FBI also uses Stingrays for cell phone tracking, sometimes with or without a warrant because the technology operates like pen-registers and trap-and-trace devices, collecting non-content-based information.[316]

The Federal government also collects information through the National Counterterrorism Center (NCTC) collecting airline passenger information and surveillance data over the nations borders.[317] The U.S. Treasury collects cash transaction reporting and Suspicious Activity Reporting data.[318] State and local law enforcement are also implementing technologies to track people entering and exiting cities,[319] and may in the future start tracking persons using electronic toll collections and electronic transit card transactions.[320]

[310] Brian T. Yeh & Charles Doyle, Cong. Research Serv., RL 33332, USA Patriot Improvement and ReAuthorization Act of 2005: A Legal Analysis 10-11 (2006).

[311] *Id.*

[312] 334 F.Supp.2d 471 (SDNY 2004). However, the SDNY's declaration of the NSL statute as unconstitutional as applied to ISPs and the gag order as unconstitutional on its face were later declared moot. *Doe v. Gonzalez*, 449 F.3d 415 (2d Cir. 2006).

[313] No. C 11-02173 SI, 2013 WL 1095417 (N.D. CA March 14 2013).

[314] Ryan Singel, *Point, Click ... Eavesdrop: How the FBI Wiretap Net Operates*, Wired Magazine (Aug. 29, 2007) http://www.wired.com/politics/security/news/2007/08/wiretap.

[315] 47 U.S.C. §1002(a) (1998).

[316] Kim Zetter, *Secrets of FBI Smartphone Surveillance Tool Revealed in Court Fight*, Wired Magazine (April 9, 2013), http://www.wired.com/threatlevel/2013/04/verizon-rigmaiden-aircard/.

[317] Julia Angwin, *U.S. Terrorism Agency to Tap a Vast Database of Citizens*, The Wall Street Journal (Dec. 13, 2012), http://online.wsj.com/article/SB10001424127887324478304578171623040640006.html.

[318] Holly Gilbert, *Treasury Department Using Advanced Analytics to Help Detect, Prevent Money-Laundering*, Security Management (April 16, 2013), http://www.securitymanagement.com/news/treasury-department-using-advanced-analytics-help-detect-prevent-money-laundering-0012366.

[319] Cara Buckley, *New York Plans Surveillance Veil for Downtown*, New York Times (July 9, 2007), http://www.nytimes.com/2007/07/09/nyregion/09ring.html?_r=2&.

[320] Nasreen Quibria, *The Contactless Wave: A Case Study in Transit Payments*, Emegerninc Payments industry Briefing, Federal Reserve Bank of Boston, 17, (2008), *available at* http://www.bostonfed.org/economic/cprc/publications/briefings/transit.pdf.

In a partnership context, the Nationwide Suspicious Activity Reporting Initiative ("SAR") is a Federal-Local partnership establishing a national capacity for gathering, documenting, processing, analyzing, and sharing suspicious activity information among federal, state and local law enforcement agencies.[321] Suspicious activity is defined as "observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity."[322] This partnership retains its importance from the 9/11 Commissions recommendation of data sharing across agencies and jurisdictions, and is enhanced by a national network of fusion centers, which are owned and operated by state and local entities with Federal support, and conduct analysis and facilitate information sharing.[323]

However, attempts at intelligence gathering, analysis and sharing partnerships have been widely criticized as being ineffective in counterterrorism investigations.[324] Furthermore, the lack of safeguards has led to the subjective elements of law enforcement and intelligence analysts to infect the potential efficacy of such systems.[325] For example, fusion centers labeled Muslim lobbyists as threats, Maryland protesters have been placed in a federal terrorism database, third party presidential candidate supporters have in the past been considered a threat.[326]

Finally, the FBI developed the Law Enforcement National Data Exchange ("N-DEx") which uses "criminal justice data from local, state, tribal, and federal agencies across the nation to quickly "connect the dots" between data that may seem unrelated."[327] The N-DEx is a Google-like search engine that combines incident and case reports, arrest reports, computer-aided dispatch calls, traffic citations, narratives, photos, supplements, booking and incarceration data, and parole/probation information.[328] This partnership is similar to the data retention and collection regime envisioned through the use of predictive analytics with one major difference: the subjectiveness of the security officials could taint the objectiveness of the data collection method similar to the criticism of fusion centers. In the predictive analytical regime, all data would be included into the database by security officials and the algorithm itself would be responsible for making the connections in which humans are currently responsible for in fusion centers, N-DEx and SAR.

Although the major concern with data retention revolve around requiring business's to retain data, this discussion is outside the scope of this article. There are two main arguments against the accumulation and retention of data. First, data

[321] The Nationwide SAR Initiative, U.S. Department of Justice, *available at,* http://nsi.ncirc.gov/.
[322] *Id. available a*t http://nsi.ncirc.gov/about_nsi.aspx.
[323] *Id.*
[324] *See generally* Torin Monahan & Neal A. Palmer, *Emerging Politics of DHS Fusion Centers*, Security Dialogue (2009), *available at* http://torinmonahan.com/papers/FC-SD.pdf.
[325] David Rittgers, *We're All Terrorists Now*, CATO Institute (Feb. 2, 2011), http://web.archive.org/web/20110415064139/http://www.cato-at-liberty.org/we%E2%80%99re-all-terrorists-now/.
[326] *Id.*
[327] N-DEx: Law Enforcement National Data Exchange, Federal Bureau of Investigation, *available at*, http://www.fbi.gov/about-us/cjis/n-dex.
[328] *Id.*

retention violates fundamental rights.[329] Second, data retention is a threat to privacy.[330]

ii. Data Accumulation and Retention Does Not Violate Fundamental Rights.

It has been argued that for the past sixty years, international human rights law has enshrined the freedom of expression, access to information, privacy of communications and presumption of innocence; creating a presumption against government intervention.[331] Central to this idea is the right of individuals to express their ideas – even controversial ones – free from government surveillance.

The reliance on publishing anonymously is widely recognized[332] and that the right to remain anonymous "enhances the free expression of information of ideas" that can be infringed upon if on-line privacy is diminished.[333] It is supported by a study that suggests fifty percent of Germans would not contact marriage counselors through telephone or emails for fear that the retention of data by ISPs would infringe upon their privacy.[334]

There is certainly no argument that government officials using the First Amendment or fundamental rights of citizens as a basis for surveillance is contrary to the ideals of the United States. There is also no argument that this often happens in the national security age.[335] But the predictive analytical regime can ensure domestic terrorist profiling is not infected with the subjective thoughts of a particular investigator. The "promise of big data is that we do what we've been doing – profiling – but make it better, less discriminatory, and more individualized."[336] Domestic intelligence and law enforcement agents would not rely on such information to infringe upon the rights of U.S. persons to engage in lawful dissent. Rather, the data retention regime would be focused on providing law enforcement with pre-investigatory leads helping them identify potential threats before the threats are realized. These leads would not only rely on radicalized associations – such membership in particular organizations or open-source web posts denoting criminal behavior – but also suspicious buying habits, suspicious tax returns, or suspicious financial transactions. The use of the data, alone, would not be used to detain, arrest, or prosecute individuals for their forum communication nor

[329] *Data Retention Mandates: A Threat to Privacy, Free Expression and Business Development*, Center for Democracy & Technology (October 2011), 9-11, https://www.cdt.org/files/pdfs/CDT_Data_Retention_Paper.pdf.
[330] *Id.* at 12.
[331] *Id.* at 9.
[332] *Id.* (citing *Solers, Inc. v. Doe*, 977 A.2d 941 (D.C. Cir. 2009)
[333] Declaration on Freedom of Communication on the Internet (Adopted by the Committee of Ministers, May 28, 2003), https://wcd.coe.int/ViewDoc.jsp?Ref=Decl-28.05.2003.
[334] *What the European Commission Owes 500 million Europeans*, European Digital Rights Institute, *available at* www.edri.org/files/Data_Retention_Conference_031210final.pdf.
[335] *Mapping Muslims: NYPD Spying and Its Impact on American Muslims*, City University of New York School of Law (March 2013), http://www.law.cuny.edu/academics/clinics/immigration/clear/Mapping-Muslims.pdf.
[336] *Id.*

their buying habits. Those actions would simply flag them as persons of interests triggering an investigation, after which they would be either cleared or detained and further prosecuted.

Furthermore, under international law, a key concept in judging the validity of any restriction on protected rights is whether the restriction is "necessary" to serve a legitimate government interest, a judgment that entails an inquiry into the proportionality and effectiveness of the restriction.[337] Social networking has changed this conception of what is necessary. Society has placed reliance on posting thoughts, ideas, actions, travel plans, and other information on open-source websites where they have no reasonable expectation of privacy. The threat of lone wolf and homegrown extremism, and the risk to human life, suggests that the use of predictive analytics, data retention, and data mining are necessary to protect the lives of innocent persons. This is further enhanced by the acknowledgment that such a regime would not markedly change the legal basis for reasonable suspicion and probable cause.

iii. Data Retention Does Expose Individuals to the Threat Of Invasions Of Privacy, Though Appropriate Safeguards Can Be Implemented To Guard Against Such Privacy Invasions.

Finally, it has been argued that data retention violates privacy rights and that for such rights to be preserved, the amount of data collected and held should be kept to a minimum.[338] Many concerns revolve around the Orwellian dystopia of 1984 - concerns of free will, fairness, justice, and the presumption of innocence.[339] Such concerns are legitimate, with the caveat that social networking may have changed things. In other words, has social networking and the sharing of seemingly private information changed how our society conceptualizes private information? Are we as a society more open to having less privacy and telling everyone what we do every waking moment of our lives or should we expect those communications to also be private? How would the legal landscape change as a result of our societal expectations – do we have a reasonable expectation of privacy in what we do outside?

As the law currently stands, people have no expectation of privacy in materials they knowingly and voluntarily expose to third parties[340] such as where

[337] *See "Regardless of Frontiers:" the International Right to freedom of Expression in the Digital Age*, Center for Democracy and Technology (April 2011), http://www.cdt.org/files/pdfs/CDT-Regardless_of_Frontiers_v0.5.pdf.

[338] *See* The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Organization for Economic Co-operation and Development (1980), *available at* http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.

[339] Viktor Mayer-Schonberger & Kenneth Cukier, *Big Data*, p. 227-28, Houghton Mifflin Harcourt (2013).

[340] *California v. Greenwood*, 486 U.S. 35, 41 (1988).

we drive,[341] our license plates, received emails,[342] called phone numbers,[343] or open fields.[344] This includes where someone travels, what people post on Facebook, websites, or Twitter. Furthermore, we do not have a reasonable expectation of privacy in Internet subscriber information.[345]

Additionally, companies store massive amounts of information about consumers such as their personal information, their buying habits, their method of payment, and others, all in the hopes of increasing the effectiveness of marketing and advertising campaigns.[346] However such data retention by private companies generally does generate the same types of concerns from privacy advocates than that of government retention of data. In fact, it can be argued that when Amazon recommends a particular product to us – based on key search terms and previous purchases – that we enjoy these analytical regimes to make our lives a lot easier. Certainly this has a lot to do with American history and our innate distrust of government; however, given the information we already give the government, their ability to store such information, the information and use of analytics by private companies and, in the homegrown terrorism age, the higher demand for security cameras in large urban environments, the line of what is private and what is not has been obliterated.

Government investigations reveal massive amounts of information relating to names, addresses, ages, banking records, travel information, and much more. While the sheer volume of information that the government can and does retain is massive, the fact that government may have this ability is of less concern than how this data is stored, who has access to it, and how long the data is retained. With government budgets ever-decreasing, some agencies have used analytics to help in their investigations.[347] The SEC and IRS undergo massive "data mining and quantitative algorithms and statistical modes" to identify anomalies in data to help investigate and prosecute financial crimes and tax abusers.[348] Why should the national security apparatus be deprived of this new technological breakthrough?

In the predictive analytical age, concerns around privacy revolve around four issues. First is nature – what kind of information would be retained. Second is time –

[341] *United States v. Knotts*, 460 U.S. 276, 281-82 (1983) ("a person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements…").

[342] *Guest v. Leis*, 255 F.3d 325 (6th Cir. 2001); *United States v. Perrine*, 518 F.3d 1196 (10th Cir. 2008).

[343] *Smith v. Maryland*, 442 U.S. 735 (1979). Although the Electronic Privacy Act, 18 U.S.C. §3121 (2001), prohibits the use of pen registers unless consent or a court order is obtained, the Patriot Act allows for the collection of such information.

[344] *Dow Chemical v. United States*, 476 U.S. 227 (1986)

[345] *United States v. Perrine*, 518 F.3d 1196 (10th Cir. 2008)

[346] *See* Kasmir Hill, *How Target Figured Out a Teen girl Was Pregnant Before Her Father Did*, Forbes Magazine (February 16, 2012, http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/.

[347] *See* Richard Satran, *What Does the IRS Know About You?*, U.S. News Money (Apr. 12, 2013), http://money.usnews.com/money/personal-finance/mutual-funds/articles/2013/04/12/what-does-the-irs-know-about-you; Charles S. Clark, *IRS and SEC Detect Fraud Patterns in Heaps of Data*, Government Executive (Oct. 16, 2012), http://www.govexec.com/technology/2012/10/irs-and-sec-detect-fraud-patterns-heaps-data/58816/.

[348] *See id.*

how long is the information going to be stored. Third is access - who should be able to access the information that is stored. Finally, is accountability – with so much data available protections must be implemented to protect access, prevent abuse, and rectify potential harms. Thus the liability of data retention is that such information is vulnerable to hackers, accidental disclosure, and other unauthorized third-party access aggravating identity theft concerns.

Safety mechanisms, encryption, and other proactive security devices must be implemented to ensure the database is not compromised; however, such a concern is not sufficient to discount the use of a potentially legitimate law enforcement tool in identifying and investigating homegrown terrorist plots. The NCTC privacy guidelines, for example, prohibit "access[ing], acquir[ing], retain[ing], us[ing], or disseminat[ing] United States person information solely for the purpose of monitoring activities protected by the First Amendment or monitoring the lawful exercise of other rights secured by the Constitution or other laws of the United States."[349]

Although a predictive analytical regime does not yet exist, the SAR and N-DEx partnerships, as well as the NCTC guidelines, allow us to understand how such information is currently retained, accessed and protected. In the N-DEx context, a security official becomes a user through the local agency within which they work – in other words a local appointed process.[350] Only such users are allowed access to the N-DEx database which reinforces the sensitive nature of the data. Furthermore, access to the database is only allowed through specialized networks and computers within the system that are allowed to access the database.[351] Sensitive information is protected by being marked as such through a color-coded system allowing the owner of the information – the agency that uploaded the data – to protect the privacy of the data.[352] Privacy concerns within the N-DEx database is enhanced by working with the FBI's Privacy and Civil Liberties Unit ("PILCU") as well as advocacy organization such as the American Civil Liberties Union and the Innocence Project.[353] Furthermore, agencies that upload information to the database are subject to the oversight of their state laws – triggering even more protections.[354]

Similar privacy protections can be implemented in the predictive analytical regime as well; with one caveat. Access would be limited to officials once a suspect is flagged for additional security, making the database more secure than it is now. For example, the data would be uploaded by a variety of local and national agencies

[349] *Guidelines for Access, Retention, Use, and Dissemination By the National Counterterrorism Center and Other agencies Of Information in Datasets Containing Non-Terrorism Information*, National Counterterrorism Center, 4, *available at* www.fas.org/sgp/othergov/intel/nctc_guidelines.pdf. *See also* http://www.nyc.gov/html/nypd/downloads/pdf/crime_prevention/public_security_privacy_guidelines.pdf

[350] N-DEx: Law Enforcement National Data Exchange, Federal Bureau of Investigation, http://www.fbi.gov/about-us/cjis/n-dex/questionsandanswers#_How_many_users.

[351] *Id.*

[352] *Id.*

[353] *Id.*

[354] *Id.*

and the algorithm would operate to find hidden connections in the data. As a result, a local and federal law enforcement agency would not have unfettered access to the data, but rather would be automatically provided that information in the file relating to a domestic terrorist plot within their jurisdiction. Therefore, it would be in the interest of local law enforcement to populate the database as early as possible to ensure connections are developed, and officials alerted, in a timely fashion.

Under this regime, the major concern is over inclusiveness and zealousness of officers. In other words, the risk that law enforcement would attempt to retrieve any and all personal information with the goal of including such information in the database for future retrieval. However, this privacy concern implicates operational considerations such as whether the information is valuable to national security.

There are two ways to address such concerns. On the one hand, the government can limit the data included in the database on the front end so as to prevent an inundation of data. However such a solution would render the database ineffective since it's data points would be artificially limited. On the other hand, the government can implement retention time tables which would require the destruction of information related to law-abiding persons within two years of data collection provided that no illicit associations, relationships or other connections are found by the algorithm within that time period. This back-end solution would ensure the database is sufficiently populated to make future predictions, while ensuring a reasonable degree of privacy. However, it should be noted that the information in the database would not be private, but rather either open-source information in which persons have no expectation of privacy or information related to law enforcement encounters – which would, in any case, be retained in files and reports by local law enforcement. In the end, data retention allows for a secondary use of the data similar to that of private companies.[355]

Today, the sheer breadth and scope of information available to individuals, companies, and governments is enormous. As society engages in more activities that limit their reasonable expectation of privacy and allow companies and government to retain information on a scale never before seen, the attraction to use such information for national security is too great. The nation must use all efforts to protect itself from homegrown terrorism, while maintaining privacy and constitutional protections Americans expect. It is within the predictive analytics regime that I believe this balance is struck.

[355] Technology companies have used this secondary approach to data to their advantage. Luis von Ahn founded Captcha to solve the problem of spam bots inundating email boxes and online forums by requiring a user to read and type hard-to-read letters. Von Ahn's successor company, ReCaptcha, found a secondary purpose for this technology by using the user's free labor to also help digitized hard to read texts. *See* Viktor Mayer-Schonberger & Kenneth Cukier, *Big Data*, p. 149-150, Houghton Mifflin Harcourt (2013).

VI. POLICY CONSIDERATIONS

The development of a predictive analytical regime would require substantive policy decisions and changes that encompass value judgments and weigh the costs of security with the benefits of liberty. First, the national security infrastructure would need to consider whether or not the creation of a domestic intelligence agency is warranted. Second, is the difference in roles between intelligence and law enforcement. Third, is the courage to develop and implement data retention technologies. Fourth, is that predictive analytics and data retention does not hinder national security objectives. Finally, are the current practical limitations of the predictive analytical regime.

This is where predictive analytics is successful, though it must be constrained in the manner discussed in this paper. That is, predictive analytics should be used as a tool to profile potential suspects – but the legal system should be careful not to allow reliance on such an algorithm to defend arbitrary detention and limitation of liberty interests without corroboration from law enforcement through traditional investigations.

A. *Creation of a Domestic Intelligence Agency is NOT Needed to Implement a Predictive Analytical Regime OR To Ensure Domestic National Security.*

The 9/11 Commission considered and rejected calls for the development of an American domestic surveillance counterpart to the UK's MI-5.[356] The Commission's rejection relied on the government implementing its other recommendations to share national security information.[357] Among the recommendations the Commission advised the government, was the creation of the National Counterterrorism Center ("NCTC") that would "oversee counterterrorism intelligence work, foreign and domestic, and the creation of the Office of the Director of National Intelligence ("ODNI") whose office would "set and enforce standards for collection, processing, and reporting of information."[358]

However this structure continues to be fallible. The NCTC was criticized for failing to identify the threat posed by the 2009 Christmas Day bomber.[359] This failure, echoing similar concerns to those after the September 11, 2001 terrorist attacks,[360] failed to connect NSA intercepts of al Qaeda operatives in Yemen talking about using a Nigerian man for an attack with a warning from Abdulmuttalab's father about his son's extremist views.[361] This failure is not only one of data sharing, but also possibly one of culture and values. Each of the intelligence agencies has

[356] National Commission on Terrorist Attacks upon the United States. (Philip Zelikow, Executive Director; Bonnie D. Jenkins, Counsel; Ernest R. May, Senior Advisor). *The 9/11 Commission Report*. p.423. New York: W.W. Norton & Company, 2004.

[357] *Id.* at 432.

[358] *Id.* at 423.

[359] Scott Shane, *Shadow of 9/11 Is Cast Again*, The New York Times (Dec. 30, 2009). http://www.nytimes.com/2009/12/31/us/31intel.html?_r=0.

[360] *Id.* (noting Thomas H. Kean, chairman of the 911 Commission).

[361] *Id.*

developed it's own value system that differs from all the others. For example, the CIA values intelligence whereas the FBI values law enforcement and rule of law.

Despite this failure, the creation of a domestic surveillance agency – and added bureaucracy - is unwarranted, especially in an age where predictive analytics supports the national security infrastructure. If each agency is required to add into a national intelligence database, information relating to domestic and international terrorist plots and suspects, the failure to identify the Christmas Day bomber may not have occurred.

The new ODNI structure of the Intelligence Community would not need to be changed in implementing predictive analytics. In fact, it is uniquely situated to coordinate, plan, and structure such a database for true interagency cooperation by virtue of its mandate to lead intelligence integration.[362] Furthermore, the database would bypass any agency cultural issues which may prohibit true data sharing because the agencies would be required to populate the database with any and all information relating to the national security of the United States.

Finally, the creation of a domestic intelligence agency is ill founded for the purpose of combatting homegrown terrorism due to the nature of the threat. Domestic threats are not necessarily threats involving foreign agents or powers.[363] As discussed earlier they may involve a variety of ideologies, religions, or viewpoints whereby individuals may become radicalized in a lone wolf scenario. Furthermore, domestic terrorist threats often involve traditional violations of crime such as fraud and identity theft. It is because domestic terrorist incidents often intersect with law enforcement that the FBI is uniquely situated to identify, investigate and prosecute such threats.

As a result, this discussion parallel's the 9/11 Commission's five-point rejection of the creation of a domestic intelligence agency.[364] Included in the 9/11 Commission report is the focus on data sharing as necessary to combat terrorist threats. Given the recent failures and practical agency-culture limitations that may exist, predictive analytics and a national intelligence database may bypass such concerns in the future.

B. *An Intelligence-Driven Law Enforcement Regime is Needed to Protect The Nation From Homegrown Threats.*

Before the September 11, 2001 terrorist attacks, the focus on counterterrorism investigations revolved around law enforcement with support from intelligence agencies. In the wake of the attacks, the intelligence community took center stage and the law enforcement community playing only a supporting, if any, role in the investigation and combatting of terrorist incidents. However, as

[362] *Mission, Vision & Goals*, Office of the Director of National Intelligence, http://www.odni.gov/index.php/about/mission

[363] 50 U.S.C. §1801(b)(1)(C) (2010)

[364] National Commission on Terrorist Attacks upon the United States. (Philip Zelikow, Executive Director; Bonnie D. Jenkins, Counsel; Ernest R. May, Senior Advisor). *The 9/11 Commission Report.* p.423-24. New York: W.W. Norton & Company, 2004.

discussed previously, the changing nature of the threat from foreign sources to homegrown terrorism demands a comparable change in the response and tools available to security officials. This 4GW threat and the development of predictive analytics demands a true integration of the intelligence infrastructure with law enforcement mechanisms to ensure threats are identified before they are realized. Furthermore, the lack of a law enforcement emphasis in terror investigations and prosecutions has largely been anemic resulting in "little reliable information."[365] In fact, because of the lack of law enforcement emphasis, convictions have been overturned due to sloppy or fraudulent prosecutions or have not even gone to trial.[366] This problem is evident in the Britain as well as they dealt with the prosecution of Abu Hamza.[367]

As discussed earlier, homegrown terrorism, and efforts to support it often encompass other crimes such as fraud, smuggling, identity theft, and money laundering.[368] These crimes, although possibly revealed through intelligence mechanisms is better suited for the local, on the ground resources of the law enforcement community with support from the FBI. Furthermore, domestic and international terrorists do not respect boundaries that are traditional jurisdictional divides between intelligence and law enforcement agencies. It is for this reason that intelligence agencies, along with their information gathering capacity, must also play a key role.

As a result, there must be collaboration among the local, state, and federal law enforcement agencies along with the federal, and global, intelligence agencies in combatting terrorism. Although as previously noted, there are practical limitations that exist for voluntary sharing of national security information, within a predictive analytical regime, this collaboration would be to require uploading information relating to domestic and international threats to a national security database.

However this regime also demands a collaborative approach to the culture and investigation of homegrown terrorist incidents. In the law enforcement context, police and the FBI seek to find all the evidence they can to identify perpetrators and investigate potential leads of future threats under the auspices of a future prosecution. On the other hand, intelligence agencies are focused on the same sets of issues, but under the auspices of developing intelligence and protecting the nation against future threats.

But, the failure of United States to prevent the September 11, 2001 terrorist attacks was not solely data sharing, but rather a failure of integration.[369] Provided

[365] Karen J. Greenberg, *European Counterterrorism and Its Implications for the U.S. War on Terror*, in PROSECUTING TERRORISM: THE GLOBAL CHALLENGE, 3, The NYU Review of Law and Security, (Summer 2005).

[366] *Id.* (citing the Terrorist Trial report Card, Center on Law and Security, 2004).

[367] Pete Clark, *The British Experience with Counterterrorism*, in PROSECUTING TERRORISM: THE GLOBAL CHALLENGE, 16, The NYU Review of Law and Security, (Summer 2005).

[368] Colleen McCue, *Datamining and Predictive Analytics: Battlespace Awareness of the War on Terrorism*, Defense Intelligence Journal; 13-1&2 (2005), 47, 48.

[369] National Commission on Terrorist Attacks upon the United States. (Philip Zelikow, Executive Director; Bonnie D. Jenkins, Counsel; Ernest R. May, Senior Advisor). *The 9/11 Commission Report*. p.416-417. New York: W.W. Norton & Company, 2004.

there is an integrated data accumulation and analysis infrastructure combined with an understanding that law enforcement tools and cultures are necessary to identify violations of crime that, combined with intelligence reveal homegrown threats, predictive analytics can accurately model complex interactions, associations, and relationships and use these models to identify and characterize unknown relationships to make reasonable predictions of future events.[370]

C. *Collection, Sharing and Retention of Data.*

Within the context of the intelligence-law enforcement divide is the development of a national security database and automatic sharing infrastructure that would facilitate a predictive analytics algorithm. Both American and European experts agree that the future of terrorism will likely come from less organized, smaller groups of terrorists whose attacks are on a smaller scale than September 11, 2001.[371]

The 9/11 Commission noted the importance of data sharing, which was why many of their recommendations involved the creation of the ODNI and the NCTC to facilitate such actions.[372] The 2001 attacks, in their view, was a failure of the data sharing capabilities within the intelligence community.[373] Although we may demand voluntary sharing of national security information, in the predictive analytical age, this voluntariness may be counterproductive and artificially limit the data points with which an algorithm can rely.[374]

In this new collaborative effort, the President has authorized, through Executive Order 13388, the sharing of terrorism information and required "that agencies place the highest priority on the interchange of terrorism information in order to strengthen the effective conduct of United States counterterrorism activities."[375] Furthermore, the authority for the development of a national security database resides in the President's position as Commander in Chief of the armed forces.[376] This authority is further supported by Congress through the National Security Act of 1947, as amended, which recognized that the "NCTC must have

[370] Colleen McCue, *Datamining and Predictive Analytics: Battlespace Awareness of the War on Terrorism*, Defense Intelligence Journal; 13-1&2 (2005), 47, 48.

[371] Karen J. Greenberg, *European Counterterrorism and Its Implications for the U.S. War on Terror*, in PROSECUTING TERRORISM: THE GLOBAL CHALLENGE, 3, The NYU Review of Law and Security, (Summer 2005).

[372] National Commission on Terrorist Attacks upon the United States. (Philip Zelikow, Executive Director; Bonnie D. Jenkins, Counsel; Ernest R. May, Senior Advisor). *The 9/11 Commission Report,* 403-14. New York: W.W. Norton & Company, 2004.

[373] *Id.* at 416-19.

[374] For example, in the case of Abdulmutallab, the threat poses by the bomber has been identified as a failure of sharing of national security information. *See* Claire Newell, et. al., *Umar Farouk Abdulmutallab: One Boy's Journey to Jihad*, The Sunday Times (London) (Jan. 3, 2010), http://www.timesonline.co.uk/tol/news/world/middle_east/article6974073.ece.

[375] *Guidelines for Access, Retention, Use, and Dissemination By the National Counterterrorism Center and Other agencies Of Information in Datasets Containing Non-Terrorism Information*, National Counterterrorism Center, 2, *available at* www.fas.org/sgp/othergov/intel/nctc_guidelines.pdf.

[376] U.S. CONST. art II, § 2.

access to a broader range of information than it has primary authority to analyze and integrate if it is to achieve its missions."[377] Furthermore, in the post-9/11 security infrastructure, Section 102A(b) of the National Security Act of 1947, as amended, provides that "[u]nless otherwise directed by the President, the Director of National Intelligence shall have access to all national intelligence and intelligence related to the national security which is collected by any federal department, agency, or other entity, except as otherwise provided by law or, as appropriate, under guidelines agreed upon by the Attorney General and the Director of National Intelligence."[378]

In this new age, the NCTC would continue to "serve as the primary organization in the United States Government for analyzing and integrating all intelligence possessed or acquired by the United States Government pertaining to terrorism and counterterrorism."[379] Any challenges to the authorization of data collection for national security purposes would likely fall within the state secrets privilege.

However, retention of national security information does not change if the subject of that threat is a U.S. person or not. In that context, the intelligence-gathering agency would not be the CIA, NSA or other intelligence entity, but rather the FBI under it's current mandate as an "intel-driven national security and law enforcement agency" or the local law enforcement.[380] Under that law enforcement regime, the data is retained already, through the NCIC and other databases that even now allow law enforcement to link past crimes, fingerprints, and methods to identify and help investigate current crimes.[381] It is under this new mandate that the NCTC and the FBI would provide a unique and powerful team to identify and investigate homegrown terrorism. But as discussed throughout this paper, local law enforcement possesses the necessary on the ground support for data accumulation.

For example, after the 2001 terrorist attacks, New York implemented the Lower Manhattan Security Initiative, which will, upon completion, resemble London's Ring of Steel.[382] The authority for this initiative is rooted in the NYPD's plenary power to preserve the public peace and prevent crime as well as "regulate, direct, control and restrict the movement" of vehicle traffic.[383] This initiative will encompass an extensive web of cameras and roadblocks designed to detect, track, and deter terrorists.[384] As New York has implemented this initiative, the next phase

[377] *Guidelines for Access, Retention, Use, and Dissemination By the National Counterterrorism Center and Other agencies Of Information in Datasets Containing Non-Terrorism Information*, National Counterterrorism Center, 2, *available at* www.fas.org/sgp/othergov/intel/nctc_guidelines.pdf.

[378] *Id.*

[379] *Id.* at 1.

[380] *See About Us*, Federal Bureau of Investigation, http://www.fbi.gov/about-us.

[381] *National Crime Information Center*, Federal Bureau of Investigation, *available at*, http://www.fbi.gov/about-us/cjis/ncic.

[382] Cara Buckley, *New York Plans Surveillance Veil for Downtown*, New York Times (July 9, 2007), http://www.nytimes.com/2007/07/09/nyregion/09ring.html?_r=2&.

[383] Chapter 18 §435(a) of the New York City Charter.

[384] Cara Buckley, *New York Plans Surveillance Veil for Downtown*, New York Times (July 9, 2007), http://www.nytimes.com/2007/07/09/nyregion/09ring.html?_r=2&.

is currently underway with the installation of license plate scanners.[385] These scanners will photograph all license plates and vehicle types entering and exiting Manhattan.[386] The data from the video is stored for thirty days, can be extended by the Deputy Commissioner of Counterterrorism and data from the license plate scanners are stored for five years. [387] This data can be used as a key post-event investigatory tool. However, these scanners can also be used as a preventative measure, but this would require data sharing and retention collaboration between other States, rental companies, and foreign state motor vehicle associations. In such a collaborative environment, the scanners would track, in real time, license plates of cars that were reported stolen or cars with license plates that are not registered to it. In the national security context, if this collaborative environment existed, it is possible that Abdulmuttalab would have been identified prior to him parking his Nissan Pathfinder because the vehicle had stolen license plates.[388]

The international experience is instructive on the development of a centralized data collection initiative. For example, the French established a highly centralized system for collecting data through criminal investigations.[389] Furthermore, Canada has the Canadian Security Intelligence Service (CSIS) which is responsible of collecting, analyzing, reporting, and disseminating intelligence threats regarding national security and conducting operations within and outside the nation.[390] Although jurisdictional conflicts continue, the centralized data system seems to have worked for both the French and Canadians in their ability to prevent, investigate, and successfully prosecute terrorists in their country.[391]

Finally, a predictive analytical regime would necessarily need to consider the possibility of developing a global information-sharing database to increase the effectiveness of a predictive analytical algorithm. The value of such a project would to ensure that security and intelligence agencies across the global have the necessary information to combat terrorists from entering their jurisdiction. In the current context, a global database and sharing infrastructure would have prevented Abdulmuttalab from receiving a multiple-entry visa into the United States due to concerns from the UK about Abdulmuttallab's extremist views and ties.

[385] Matt Sledge, *NYPD License Plate Readers Will Be Able to Track Every Car Entering Manhattan*, The Huffington Post (Mar. 13, 2013), http://www.huffingtonpost.com/2013/03/13/nypd-license-plate-readers_n_2869627.html.

[386] *Id.*

[387] *Public Security Privacy Guidelines*, New York City Police Department (Apr. 2, 2009), http://www.nyc.gov/html/nypd/downloads/pdf/crime_prevention/public_security_privacy_guidelines.pdf

[388] Claire Newell, et. al., *Umar Farouk Abdulmutallab: One Boy's Journey to Jihad*, The Sunday Times (London) (Jan. 3, 2010), http://www.timesonline.co.uk/tol/news/world/middle_east/article6974073.ece.

[389] Karen J. Greenberg, *European Counterterrorism and Its Implications for the U.S. War on Terror*, in PROSECUTING TERRORISM: THE GLOBAL CHALLENGE, 3, The NYU Review of Law and Security, (Summer 2005).

[390] *Role of the CSIS*, Canadian Security intelligence Service, http://www.csis-scrs.gc.ca/bts/rlfcss-eng.asp.

[391] *Id.*

However, to be successful such a regime would necessarily have to consider nine principles set forth by INTERPOL Secretary General Ronald Noble.[392] First, countries have an obligation to "prevent dangerous criminals from entering their country," which will have important global consequences of enhancing domestic security.[393] Second, countries have a responsibility to warn other countries about individuals presenting a potential threat.[394] Noble notes the practical limitations of the voluntary sharing of national security information; however, such concerns may be mitigated with the development of a global database and the use of predictive analytics to predict future attacks.[395] Third, although it is impossible to create a global arrest warrant, this fact must not preclude countries from sharing data relating to *known* individuals wanted for terrorism.[396] Fourth, police should have the means to communicate globally and securely.[397] Fifth, countries have an obligation to proactively and internationally report any travel documents that are stolen or blank.[398] Sixth, every country should have security staff that can immediately query international databases and respond to immediate needs in real time.[399] Seventh, countries should ensure that their police officers are trained in communication technology and international databases.[400] Eighth, countries should ensure that membership in a terrorist organization constitutes a criminal offense.[401] Finally, when a terrorist attack occurs, countries should invite International Incident Response Teams to the location and allow them to assist with the investigations.[402]

Although these principles are devoted to international responses to terrorist incidents that occur with foreign or international ties, they offer guiding principles for the need for international and cross-jurisdictional sharing of national security information, cross-jurisdictional investigations, and codifying international obligations of potential future threats. Adding such information into a national or global database combined with a necessary algorithm, predictive analytics would enhance national security in a manner consistent with its political and legal obligations.

[392] Ronald Noble, *Terrorism and the Law: The Global Challenge*, in PROSECUTING TERRORISM: THE GLOBAL CHALLENGE, 12-13, The NYU Review of Law and Security, (Summer 2005).
[393] *Id*. at 12
[394] *Id.*
[395] *Id.*
[396] *Id.*
[397] *Id.* at 13.
[398] *Id.*
[399] *Id.*
[400] *Id.*
[401] *Id.*
[402] *Id.*

D. *Predictive Analytics and Data Retention Does Not Hinder National Security Objectives.*

National security demands that officials have access to timely, coherent, and actionable information. It is suggested that large-scale data storage decreases the reliability and integrity of the data resulting in longer delays in data coherence[403]

However, this is not the case in a predictive analytical regime. National security officials need access to a variety of "messy" data points to quickly and efficiently track previously unknown threats.[404] "[I]n some cases big and messy can even be beneficial, since when we tried to use just small, exact portion of the data, we ended up failing to capture the breadth of detail where so much knowledge lies."[405]

As in the previous examples, if a person engages in a variety of suspicious purchases of materials, which if combined in appropriate proportions, would result in the formation of an IED, security officials have limited options without an automatic data retention and collection system. They can either wait until the suspect makes a mistake by revealing their intention, the suspect engages in a criminal action such as identity theft or fraud, an informant reveals the plot to law enforcement, or the threat is carried out and an investigation ensues. As a result, although information relating to buying habits of a particular person likely would not, reveal with certainty, the presence of criminal intent, it would allow security officials to investigate suspicious activity to determine whether or not a threat exists.

This is similar to what the FBI engages in during the SAR Initiative except that in the predictive analytical context, this information would not rely on the voluntary sharing of information. Rather it would rely on an automatic sharing of information relying on an algorithm to recommend to law enforcement the presence of national security concerns.

Thus, predictive analytics would not hinder national security objectives, but better utilize national security resources efficiently, and remove subjective elements that may inappropriately and discriminatorily limit their search parameters.[406]

E. *Practical Limitations*

Finally, it goes without saying that there are practical limitations to the implementation of a predictive analytical regime. First, the technology must develop to the idea. In other words, the technology to develop an algorithm to predict future

[403] *Data Retention Mandates: A Threat to Privacy, Free Expression and Business Development*, Center for Democracy & Technology (October 2011), 8-9, https://www.cdt.org/files/pdfs/CDT_Data_Retention_Paper.pdf.

[404] *See* Viktor Mayer-Schonberger & Kenneth Cukier, *Big* Data, p. 287, Houghton Mifflin Harcourt (2013).

[405] *Id.*

[406] *See* Amy Davidson, *The Saudi Marathon Man*, The New Yorker (April 17, 2013), www.newyorker.com/online/blogs/comment/2013/04/the-saudi-marathon-man.html.

behavior and flag potential suspects is in its infancy and needs to be developed further before it can be used in an effective manner to flag potential suspects in homegrown terrorism.[407]

Second, the government would have to develop the capacity to store massive amounts of data and employ the resources and human intelligence to develop, analyze, and manage the data in a manner consistent with the Constitution and effectiveness to protect national security.

Third, as the capacity for data retention and accumulation develops, the agencies would have to ensure they have the capacity to develop legitimate leads and follow-up their investigations with the necessary resources so as not to miss legitimate threats to national security.

Fourth, in the surveillance context, the government would have to ensure all the surveillance video and pictures are stored in the same format for easy dissemination and review by the algorithm.

Fifth, although the President would be able to implement such a data retention program within his powers as commander in chief of the armed forces, Congressional authorization would be necessary to appropriate the necessary funds.

Sixth, the States and local law enforcement agencies would have to be involved in the national security infrastructure which triggers jurisdictional, ego, and communication issues inherent as these agencies fight each other for additional money from the States and Congress.

Finally, Americans would have to accept a greater amount of government surveillance and weigh such surveillance with their liberty and privacy interests. If communicated in an appropriate manner, it is likely that predictive analytics could garner support from many in civil society; however, protections of the data, access to the data, use of the data, and accountability of the data would have to be implemented balancing national security and civil liberties concerns.

VII.CONCLUSION

The comparison between predictive analytics and the German Stasi[408] or Orwell's 1984[409] is overstated due simply to the idea of increased surveillance. However, in the homegrown terrorism age, society must make value judgments and weigh the costs of security with the benefits of liberty. As New York City continues it's Lower Manhattan Security Initiative, with the expectation of adding more cameras and scanners, [410] society has seemed to accept some level of increased

[407] *See* Beth Pearsall, *Predictive Policing: The Future of Law Enforcement?*, National Institute of Justice Journal 266, p.1 (June 2010), *available at*, http://www.nij.gov/journals/266/predictive/htm; *Police Warm to Predictive Analysis Crime Fighting Tools*, Homeland Security Wire (Sept. 22, 2010), http://www.homelandsecuritynewswire.com/police-warm-predictive-analysis-crime-fighting-tools?page=0,0 (describing the CRUSH program in Memphis Tennessee).

[408] *See* Viktor Mayer-Schonberger & Kenneth Cukier, *Big* Data, p. 226, Houghton Mifflin Harcourt (2013)

[409] *Id.* at 229.

[410] Cara Buckley, *New York Plans Surveillance Veil for Downtown*, New York Times (July 9, 2007), http://www.nytimes.com/2007/07/09/nyregion/09ring.html?_r=2&.

surveillance in their daily lives in the hopes that future terrorist attacks will be averted.

But the use of technology for security purposes and the implications on liberty interests must not shield society's eyes to the benefits of such technology with implemented protections. Technology changes the law and the law must change with it. The advent of blogs, data storage and other technology has changed the growth of the First Amendment. Similarly, the voluntary exposure of information and the destruction of privacy expectations as a result, may have provided the court with fodder to continue its *Katz* analysis in the technology age. However, there is also the implication that technology may change Fourth Amendment analysis to encompass a totality of the circumstances standard.[411] IN fact, predictive analytics may be so successful precisely because of the concerns of privacy and civil liberty advocates.

The value of predictive analytics in the national security context is in its use as a tool to profile potential suspects. That is, with the development of a national, or global database, the algorithm would data mine information flagging persons of interest for future investigation, absent subjectiveness and discrimination. However, such a system must not be sufficient to arbitrarily detain or prosecute a suspect. As a result, the predictive analytical tool should be viewed as an additional tool for law enforcement - taking the place of an informant, anonymous tip, or a mistake of the suspect – in their ongoing investigation. If implemented in this manner, the use of predictive analytics to combat homegrown terrorism would not run afoul of the Fourth Amendment and would ensure the effective use of limited security resources.

[411] *See* 132 S.Ct 945, 964 (2012) (Alito, J., concurrence); *id*. at 955 (Sotomayor, J., concurrence).