

# CAN WE FIND AND STOP THE “JIHAD JANES”?

*Diane Webber\**

## TABLE OF CONTENTS

I. INTRODUCTION .....	91
II. THE UNITED KINGDOM .....	96
A. The Tools .....	99
B. Physical Searches .....	101
C. Technological Surveillance .....	102
1. Interception of Communications.....	102
2. Surveillance .....	105
3. Transactional Data.....	107
4. Public Surveillance .....	108
III. THE UNITED STATES.....	109
A. Human Intelligence .....	110
B. Technological Surveillance .....	111
1. Domestic Surveillance .....	111
2. Foreign Surveillance.....	113
3. Transactional Information.....	118
4. Public Surveillance .....	119
IV. A GAP IN THE ARMORY?.....	121
V. CONCLUSION .....	123

## I. INTRODUCTION

“The threats we face are becoming more diverse and more dangerous with each passing day.”<sup>1</sup>

---

\* Solicitor of the Senior Courts of England and Wales; L.L.B. (Univ. of London); L.L.M. (Georgetown Univ.). The author would like to thank Professor James W. Zirkle for his comments as well as John Webber, Daniel Webber, and Katie Hyman for all their encouragement and support.

<sup>1</sup> *Securing America's Safety: Improving the Effectiveness of Anti-Terrorism Tools and Inter-Agency Communication: Hearing Before the S. Comm. on the Judiciary*, 111th Cong. (2010) (statement of Robert S. Mueller III, Director, Federal Bureau of Investigation)

Colleen LaRose, an unassuming, pint-sized, blue-eyed, blonde from Philadelphia first attracted the attention of law enforcement personnel in 2007 when she commented on YouTube, under the name “JihadJane,” that she was “desperate to do something somehow to help” suffering Muslim people.<sup>2</sup> In addition to posting increasingly agitated messages on various web sites about waging “violent jihad,” she wrote of jihad in several emails to individuals in the United States, Europe, and South Asia. These messages were monitored by U.S. and Swedish authorities, and led to her indictment on March 9, 2010 on terror charges, including conspiracy to murder a Swedish cartoonist who drew a satirical picture featuring the head of the prophet Muhammad on the top of a dog’s body.

Another American woman, Jamie Paulin-Ramirez, a trainee nurse from Colorado, converted to Islam and moved to Ireland. She was detained by authorities in Waterford, Ireland, in connection with the same terror plot, but, subsequently, was released.<sup>3</sup>

These two female American citizens, whose appearance and passports allow them to blend into Western society, represent “one of the worst fears” of the intelligence and FBI analysts who work to identify terrorist threats.<sup>4</sup> In the United States there are conflicting views about the scale of homegrown terrorism. Time Magazine reports that “while homegrown Islamic terrorism is a serious issue, it remains a limited problem.”<sup>5</sup> The article cites a report whose authors interviewed 120 Muslims in four American cities.<sup>6</sup> The report concluded that over the last eight years the record contains “relatively few examples of Muslim Americans

---

[hereinafter Mueller 2010 Statement], available at <http://www.fbi.gov/congress/congress10/mueller012010.htm>.

<sup>2</sup> See, e.g., Carrie Johnson, *JihadJane, an American Woman, Faces Terrorism Charges*, WASH. POST (Mar. 10, 2010), <http://www.washingtonpost.com/wp-dyn/content/article/2010/03/09/AR2010030902670.html>; Ed Pilkington, *Colleen LaRose: All-American Neighbor or Terrorist Jihad Jane?*, GUARDIAN, (Mar. 10, 2010), <http://www.guardian.co.uk/world/2010/mar/10/colleen-la-rose-jihad-jane-terrorism-arrest>.

<sup>3</sup> Ivan Moreno, *Jamie Paulin-Ramirez Held in Connection with Plot to Assassinate Swedish Cartoonist*, HUFFINGTON POST (Mar. 13, 2010, 11:42 PM), [http://www.huffingtonpost.com/2010/03/13/jame-paulinramirez-held\\_n\\_497882.html](http://www.huffingtonpost.com/2010/03/13/jame-paulinramirez-held_n_497882.html).

<sup>4</sup> Johnson, *supra* note 2.

<sup>5</sup> Bobby Ghosh, *Threat of Home Grown Islamic Terrorism May Be Exaggerated*, TIME (Jan. 6, 2010), <http://www.time.com/time/nation/article/0,8599,1952009,00.htm>.

<sup>6</sup> Buffalo, N.Y.; Houston, T.X.; Seattle, W.A.; Raleigh, N.C.; and Durham, N.C. *Id.*

## 2011] CAN WE FIND AND STOP THE “JIHAD JANES”? 93

that have radicalized and turned towards violent extremism.”<sup>7</sup> It is interesting to note that what this report terms as “relatively few examples” comprises 139 acts of terrorism.<sup>8</sup>

The alleged limited scale of the problem may be borne out by New York University’s Center on Law and Security’s “Terrorist Trial Report Card,” which analyzes all terrorist trials that have taken place between September 11, 2001, and September 11, 2009.<sup>9</sup> Although it is not known precisely how many people are currently under surveillance or investigation for possible terrorist offenses in the United States, the N.Y.U. analysis cites 828 people as having been indicted in that eight-year period. Of that number, 593 indictments have been resolved with a conviction rate of 88.2%. The report states that the largest contingent of defendants came from the United States, of which less than half had an alleged affiliation to a terrorist group. Most affiliations were not with radical Islamic organizations—Al Qaeda accounted for 11% of defendants. Brian Jenkins of RAND has also researched this. He states that of 125 alleged homegrown terrorists indicted between 2001 and 2009, 42 of them were indicted during 2009—indicating a steep rise at the current end of the period.<sup>10</sup>

By contrast—perhaps because he knows how many investigations are ongoing—FBI Director Robert Mueller told the Senate in January 2007: “The United States homeland faces two very different threats from international terrorism: the attack planning that continues to emanate from core al Qaeda overseas and the threat posed by homegrown, self-radicalizing groups and individuals—inspired, but not led by al Qaeda—who are already living in the U.S.”<sup>11</sup> More recently, Bruce Riedel, a scholar at the Brookings Institute noted, “[T]he trend we’ve seen in the last year

---

<sup>7</sup> DAVID SCHANZEN, CHARLES KURZMAN & EBRAHIM MOOSA, *ANTI-TERROR LESSONS OF MUSLIM AMERICAN COMMUNITIES* (2010), [http://www.sanford.duke.edu/news/Schanzer\\_Kurzman\\_Moosa\\_Anti-Terror\\_Lessons.pdf](http://www.sanford.duke.edu/news/Schanzer_Kurzman_Moosa_Anti-Terror_Lessons.pdf).

<sup>8</sup> *Id.*

<sup>9</sup> CTR. ON LAW AND SEC., N. Y. UNIV. SCH. OF LAW, *TERRORIST TRIAL REPORT CARD: SEPTEMBER 11, 2001- SEPTEMBER 11, 2009* (Jan. 2010), <http://www.lawandsecurity.org/publications/TTRCFinalJan14.pdf>.

<sup>10</sup> BRIAN MICHAEL JENKINS, RAND CORP., *WOULD-BE WARRIORS: INCIDENTS OF JIHADIST TERRORIST RADICALIZATION IN THE UNITED STATES SINCE SEPTEMBER 11, 2001* (2010), [www.rand.org/pubs/occasional\\_papers/2010/RAND\\_OP292.pdf](http://www.rand.org/pubs/occasional_papers/2010/RAND_OP292.pdf).

<sup>11</sup> *Global Threats to the United States and the FBI's Response: Hearing Before the S. Select Comm. on Intelligence*, 110th Cong. (2007) (statement of Robert S. Mueller III, Director, Federal Bureau of Investigation), available at <http://www.fbi.gov/congress/congress07/mueller011107.htm>.

and a half is less global terrorism and much more homegrown domestic terrorism within Muslim communities.”<sup>12</sup> Indeed, when the 109th Congress convened, the Senate Committee on Homeland Security and Governmental Affairs initiated an investigation into the threat of homegrown terrorists who are inspired by violent Islamist extremism, and, in 2008, that committee began looking into the role of the internet in the radicalization process.<sup>13</sup>

Disseminating propaganda is essential to the radicalization process. The internet has been instrumental in propagating Al Qaeda messages of hate to thousands of violent Islamist web sites and many chat rooms.<sup>14</sup> Indeed, “the internet has accelerated the potential for this ideology to reach beyond specific communities and enables the perception of a virtual community of like-minded radicals.”<sup>15</sup>

There appears little doubt that the internet played its part in the radicalization of people like Omar Hammami, who left Alabama, where he was raised a Baptist, to become a key figure in Islamist insurgencies in Somalia,<sup>16</sup> and permanent resident Najibullah Zazi, who pleaded guilty to plotting to detonate bombs in the New York City subway.<sup>17</sup> Zazi apparently was in email contact with Jamie Paulin-Ramirez.<sup>18</sup> Zazi is also believed to have been in email contact with one Abid Naseer, in connection with the New York City subway plot. Naseer is a Pakistani terror suspect who has been detained in the United Kingdom because of

---

<sup>12</sup> Alice Fordham, *Terror Magazine's Tip: Make a Bomb in Mom's Kitchen*, THE TIMES (London), July 2, 2010, at 11.

<sup>13</sup> MAJORITY & MINORITY STAFF OF S. COMM. ON HOMELAND SEC. & GOVERNMENTAL AFFAIRS, 110TH CONG., REP. ON VIOLENT ISLAMIST EXTREMISM, THE INTERNET AND THE HOMETOWN TERRORIST THREAT (2008), [http://hsgac.senate.gov/public/\\_files/IslamistReport.pdf](http://hsgac.senate.gov/public/_files/IslamistReport.pdf).

<sup>14</sup> *Id.* at 15.

<sup>15</sup> J. SCOTT CARPENTER, MATTHEW LEVITT, STEVEN SIMON & JUAN ZARATE, WASH. INST. FOR NEAR E. STUDIES, FIGHTING THE IDEOLOGICAL BATTLE: THE MISSING LINK IN U.S. STRATEGY TO COUNTER VIOLENT EXTREMISM, 1 (2010), [http://api.ning.com/files/GW4uSRdwPCRw7QHwfX0REzcSTVesjCjZseID\\*K9KxsGcoBtdoRCovk1r413kgdsANvKKpIqDz23Fovl\\*fk6wwVhoOfX-OIOR/StrategicReport06.pdf](http://api.ning.com/files/GW4uSRdwPCRw7QHwfX0REzcSTVesjCjZseID*K9KxsGcoBtdoRCovk1r413kgdsANvKKpIqDz23Fovl*fk6wwVhoOfX-OIOR/StrategicReport06.pdf).

<sup>16</sup> Andrea Elliott, *The Jihadist Next Door*, N.Y. TIMES MAG., Jan. 27, 2010, at 26-35, available at <http://www.nytimes.com/2010/01/31/magazine/31Jihadist-t.html>.

<sup>17</sup> See, e.g., Jason Ryan, Aaron Katersky & Mark Schone, *Zazi Pleads Guilty to Terrorism Charges*, ABC NEWS (Feb. 22, 2010), <http://www.abcnews.go.com/Blotter/najibullah-zazi-pleads-guilty-terrorism-charges/story?id=9911713>.

<sup>18</sup> Anti-Defamation League, “*Jihad Jane*” *Indicted on Terror Charges in Pennsylvania*, [http://www.adl.org/main\\_Terrorism/jihad\\_jane\\_indictment.htm](http://www.adl.org/main_Terrorism/jihad_jane_indictment.htm) (last updated May 11, 2010).

## 2011] CAN WE FIND AND STOP THE "JIHAD JANES"? 95

his alleged involvement with a bomb plot in the United Kingdom in 2009. The United States is currently seeking his extradition from the United Kingdom in connection with the New York City subway bomb plan.<sup>19</sup>

However debatable the scale of the homegrown radicalized Islamic terrorism may be, it seems beyond doubt that "the threat of domestic terror . . . is alive and well"<sup>20</sup> in the United States, and its flames are fanned by the internet.

There have been three significant recent changes in the United States relating to homegrown terrorists. First, there is the involvement of U.S. citizens in terror acts overseas. These include: (1) David Coleman Headley, who participated in the Mumbai atrocity;<sup>21</sup> (2) five men from Virginia, who traveled to Pakistan to allegedly fight U.S. soldiers in Afghanistan;<sup>22</sup> and (3) Mohammed Alessa and Carlos Almonte, two New Jersey men who sought to become members of an Islamic group in Somalia.<sup>23</sup>

Second, Al Qaeda is seeking to recruit people who lack criminal records and known ties to terrorist groups. As CIA Director Leon Panetta put it: "How many other Zazis are there—the people who have a clean record who suddenly, for some crazy reason, decide to get involved in jihad?"<sup>24</sup> Almost in answer to Panetta's question, Faisal Shahzad, a Pakistani-born U.S. citizen, attempted to detonate a car bomb in Times Square in New York City in May 2010.<sup>25</sup>

Third, there has been the radicalization of Western-looking people who blend in with those around them. According to

---

<sup>19</sup> Sean O'Neill, *Terror Suspect 'Linked to New York Plot,'* THE TIMES (London), July 8, 2010, at 31.

<sup>20</sup> *Domestic Terrorism in the Post-9/11 Era*, FEDERAL BUREAU OF INVESTIGATION (Sept. 7, 2009), [www.fbi.gov/page2/sept09/domesticterrorism090709.html](http://www.fbi.gov/page2/sept09/domesticterrorism090709.html).

<sup>21</sup> Carrie Johnson, *U.S. Citizen Admits Role in Mumbai Siege*, WASH. POST, Mar. 19, 2010, at A16.

<sup>22</sup> Jeremy Markon, Karin Brulliard & Rizwan Mohammed, *Pakistan Charges 5 N. Va. Men in Alleged Terror Plot*, WASH. POST (Mar. 18, 2010), available at <http://www.washingtonpost.com/wp-dyn/content/article/2010/03/17/AR2010031700430.html>.

<sup>23</sup> Richard Pérez-Peña & James Barron, *Two New Jersey Men in Terrorism Case Go Before a Judge*, N. Y. TIMES, (Jun. 7, 2010), available at <http://www.nytimes.com/2010/06/08/nyregion/08terror.html>.

<sup>24</sup> Joby Warrick & Peter Finn, *CIA Director Says Attacks Have Hobbled al-Qaeda*, WASH. POST, (Mar. 18, 2010), available at <http://www.washingtonpost.com/wp-dyn/content/article/2010/03/17/AR2010031702558.html>.

<sup>25</sup> *Times Square Car Bomb Suspect Faces Terrorism Charges After Admitting to Plot*, FOXNEWS (May 4, 2010), [www.foxnews.com/us/2010/05/04/pakistani-american-arrested-times-square-plot/html](http://www.foxnews.com/us/2010/05/04/pakistani-american-arrested-times-square-plot/html).

Assistant Attorney General for National Security David Kris, the Jihad Jane indictment, “which alleges that a woman from suburban America agreed to carry out murder overseas and to provide material support to terrorists, underscores the evolving nature of the threat we face.”<sup>26</sup>

This article will show that on both sides of the Atlantic, similar problems exist of homegrown terrorism and radicalization, with the internet having a huge impact on these issues. The article will examine the tools the United States and the United Kingdom have to find and stop potential homegrown terrorists from perpetrating catastrophic acts of terror. In Part I, U.K. law is discussed. In Part II, U.S. law is reviewed. In Part III, I highlight one particular area where I have found what I believe to be a gap in U.S. Title III law, and I set out some suggestions to resolve this problem.

Finally, there is an assessment of the differences between U.S. and U.K. law. I show that law enforcement personnel in the United Kingdom are able to use the tools to prevent terrorist acts more easily (although not necessarily more effectively) than their U.S. counterparts. After reviewing the scope and effectiveness of the tools available to each country, I reach the conclusion that despite the fact that each country has an impressive array of tools to thwart the homegrown terrorist, once he has been identified as a terror suspect, neither country has yet cracked the problem of finding the potential terrorist in the first place.

## II. THE UNITED KINGDOM

“Terrorists do not fall from the sky. They emerge from a set of strongly held beliefs. They are radicalized. Then they become terrorists.”<sup>27</sup>

Homegrown terrorism has been a problem in the United Kingdom for many years, starting with the explosion of bombs

---

<sup>26</sup> Press Release, U.S. Department of Justice, Office of Public Affairs, Pennsylvania Woman Indicted in Plot to Recruit Violent Jihadist Fighters and Commit Murder Overseas (Mar. 9, 2010), <http://philadelphia.fbi.gov/dojpressrel/pressrel10/ph030910a.htm>.

<sup>27</sup> Brian Michael Jenkins, *Outside Expert's View, Introduction to DAVEED GARTENSTEIN-ROSS & LAURA GROSSMAN, FOUND. FOR DEF. OF DEMOCRACIES, HOMEGROWN TERRORISTS IN THE U.S. AND U.K.: AN EMPIRICAL EXAMINATION OF THE RADICALIZATION PROCESS* (FDD Press 2009), [http://www.defenddemocracy.org/downloads/HomegrownTerrorists\\_USandUK.pdf](http://www.defenddemocracy.org/downloads/HomegrownTerrorists_USandUK.pdf).

## 2011] CAN WE FIND AND STOP THE "JIHAD JANES"? 97

placed by Irish nationalists in London in 1867.<sup>28</sup> Over the years, the source of the threat has changed: from the Irish, to Palestinians, and, since 2000, Al Qaeda related terrorism.<sup>29</sup> The London underground and bus bombing of July 7, 2005, which killed 56 and wounded 700, followed by an abortive attempt two weeks later, and an attack by doctors at Glasgow airport on June 30, 2007,<sup>30</sup> demonstrated that Islamist homegrown terrorism was alive and flourishing in the United Kingdom. A recent report notes that 69% of the 124 people convicted of terror offences since 1999 have been British nationals, many of Pakistani heritage. Half of these had no known links with any banned organizations and more than two-thirds had not been to any terror training camp.<sup>31</sup>

One recent homegrown terrorist arrest is that of Rajib Karim, who was originally from Bangladesh, but had since come to possess a British passport. He worked for British Airways as a computer expert in Newcastle and allegedly planned to take advantage of an imminent British Airways strike to work as a member of the cabin crew (the airline were looking for volunteers to keep services running during the strike). Karim appeared in court on March 10, 2010, charged with planning suicide bombings, and faces a trial in 2011.<sup>32</sup>

The annual report issued in March 2010 by the Intelligence and Security Committee, which covers the 2008-2009 period, describes the current threat as comprising four elements:

- (1) There is a serious and sustained threat from international terrorism to the UK and UK interests overseas. The level during the period of this Report was assessed as 'Severe' (it was reduced to 'Substantial' on 20 July 2009). The most significant

---

<sup>28</sup> STEVE HEWITT, *THE BRITISH WAR ON TERROR* 9 (Continuum 2008).

<sup>29</sup> PRIME MINISTER AND THE SECRETARY OF STATE FOR THE HOME DEPARTMENT, *PURSUE, PREVENT, PROTECT, PREPARE: THE UNITED KINGDOM'S STRATEGY FOR COUNTERING INTERNATIONAL TERRORISM*, HOME OFFICE, Mar. 2009, Cm. 7547, at 20-28 (U.K.) [hereinafter *CONTEST*], <http://merln.ndu.edu/whitepapers/UnitedKingdom2009.pdf>.

<sup>30</sup> HEWITT, *supra* note 28, at xviii-xix, xxiv.

<sup>31</sup> Sean O'Neill, *Five Years On, The Game Changes Again as Liberty Replaces Security*, *THE TIMES* (London), July 7, 2010, at 12 (quoting ROBIN SIMCOX, HANNAH STUART & HOURIYA AHMED, *CTR. FOR SOCIAL COHESION, ISLAMIST TERRORISM: THE BRITISH CONNECTION* (2010), [http://www.socialcohesion.co.uk/uploads/1278089320islamist\\_terrorism\\_preview.pdf](http://www.socialcohesion.co.uk/uploads/1278089320islamist_terrorism_preview.pdf)).

<sup>32</sup> Nico Hines, *Suicide Bomb Plot Suspect 'Volunteered as British Airways Cabin Crew'*, *THE TIMES* (London) (Mar. 11, 2010), <http://www.timesonline.co.uk/tol/news/uk/crime/article7058145.ece>.

threat comes from al-Qaeda and associated networks.

- (2) Northern Ireland-related terrorism continues to pose a threat. Dissident republican terrorist groups, who have rejected the 1998 Good Friday Agreement, still aspire to mount attacks in Northern Ireland and Great Britain.
- (3) The proliferation of weapons of mass destruction poses potential danger to the UK's security.
- (4) The threat from espionage remains high – several countries are actively seeking UK information and material to advance their own military, technological, political and economic programmes.<sup>33</sup>

The threat level was in fact raised again to “severe” on January 23, 2010. This means that an attack is highly likely.<sup>34</sup> More recently, Andy Hayman, former head of anti-terrorism in the Metropolitan Police commented: “We should be preparing for when the next attack happens – not if. . . . Since 9/11 in 2001, in the United Kingdom there has not been a year without either an attack or one being foiled.”<sup>35</sup>

Over the years the type of terrorist threat has changed substantially, and it is still constantly “mutating;”<sup>36</sup> however, it echoes the assessment made in the United States by Robert Mueller.<sup>37</sup> According to the United Kingdom's Strategy for Countering International Terrorism, “The current international terrorist threat is quite different from the terrorist threats we faced in the past. . . . [Terrorist groups] actively seek to recruit new members in the UK and elsewhere around the world.”<sup>38</sup> To counter this and the international terrorist threat generally, the U.K. published its CONTEST strategy in 2008 in an attempt to reduce the risk of international terrorism.<sup>39</sup> Its strategic framework has four strands:

---

<sup>33</sup> INTELLIGENCE AND SECURITY COMM., ANNUAL REPORT 2008-2009, 2010, Cm. 7807, at 4 (U.K.), <http://www.cabinetoffice.gov.uk/media/346792/isc-annualreport-0809.pdf>.

<sup>34</sup> CONTEST, *supra* note 29, at 37.

<sup>35</sup> Andy Hayman, *We Should be Preparing for When, Not If*, THE TIMES (London), July 2, 2010, at 22, *available at* <http://www.thetimes.co.uk/tto/news/uk/crime/article2583535.ece>.

<sup>36</sup> O'Neill, *supra* note 31 (quoting Assistant Commissioner of Police John Yates at Association of Chief Police Officers conference on July 2, 2010).

<sup>37</sup> See Mueller 2010 Statement, *supra* note 1.

<sup>38</sup> CONTEST, *supra* note 29, at 34.

<sup>39</sup> *Id.* ¶ 0.17.

## 2011] CAN WE FIND AND STOP THE “JIHAD JANES”? 99

- (1) *Pursue*: to stop terrorist attacks.
- (2) *Prevent*: to stop people becoming terrorists or supporting violent extremism.
- (3) *Protect*: to strengthen [the U.K.’s] protection against terrorist attack.
- (4) *Prepare*: where an attack cannot be stopped, to mitigate its impact.<sup>40</sup>

Since 2005, “the internet [has] enabl[ed] international terrorist networks to be supported from the UK. In October 2005 police arrested a Moroccan born man at his home in London from where he had set up websites . . . and published violent extremist material to incite and recruit suicide bombers in Iraq and elsewhere.”<sup>41</sup> He pleaded guilty to “inciting terrorism on the internet” at his trial in 2007.<sup>42</sup> Since then, the problems involving dissemination of terrorist-related materials via the internet has expanded enormously. CONTEST estimates that there are currently over four thousand websites “related to terrorist groups or supporting violent extremism.”<sup>43</sup> CONTEST concedes that in its aim to combat radicalization, “[t]he internet presents significant challenges for CONTEST in general and [the] *Prevent* [strand of the framework] in particular.”<sup>44</sup>

#### A. *The Tools*

In the United Kingdom, terrorism has historically been treated, and continues to be treated, as a crime to be prosecuted in regular criminal courts.<sup>45</sup> Since 2004, international terrorists have been treated in the same way as British citizens,<sup>46</sup> so there is no practical distinction in the way homegrown or international terrorists on British soil are investigated, arrested, prosecuted or treated.

The main current law in the area of detection of potential

---

<sup>40</sup> *Id.* ¶ 0.19.

<sup>41</sup> *Id.* ¶ 2.08.

<sup>42</sup> *Id.*

<sup>43</sup> *Id.* ¶ 5.14.

<sup>44</sup> *Id.* at 81.

<sup>45</sup> Terrorism Act 2000, c. 11 (U.K.), available at <http://www.legislation.gov.uk/ukpga/2000/11/contents/enacted>.

<sup>46</sup> *A (FC) and others (FC) v. Sec’y of State for the Home Dep’t* [2004] UKHL 56 (appeal taken from EWCA (Civ)) (U.K.), available at <http://www.publications.parliament.uk/pa/ld200405/ldjudgmt/jd041216/a&oth-1.htm>.

terrorists can be found in the Intelligence Services Act 1994,<sup>47</sup> the Regulation of Investigatory Powers Act 2000<sup>48</sup> (as amended), the Terrorism Act 2000,<sup>49</sup> and the Anti-Terrorism, Crime and Security Act 2001.<sup>50</sup> In the United Kingdom, law enforcement is carried out by a number of authorities: the police, and various units in the police such as the Serious Organized Crime Agency, and policing bodies such as HM Revenue and Customs. Security and intelligence services, such as MI5 and MI6, do not have law enforcement powers (i.e. they can investigate, but have no power to arrest), so their investigations must be handed over to the police when it is time to make an arrest.<sup>51</sup>

In the United States, the laws must respect the U.S. Constitution, and laws that violate it are struck down as unconstitutional. In the United Kingdom, domestic law is meant to conform to and incorporate European law. The relevant law to this discussion is the European Convention of Human Rights (ECHR),<sup>52</sup> which was incorporated into U.K. domestic law via the Human Rights Act 1998.<sup>53</sup> After exhausting the domestic court process (and some cases do end at the U.K. Supreme Court, formerly called the House of Lords<sup>54</sup>), an individual may complain to the European Court of Human Rights (ECtHR) in Strasbourg regarding the alleged violations of the European treaty, or seek clarifications about the meaning of treaty terms. If the ECtHR finds a violation of treaty rights, its scope is limited to offer redress. It can make pecuniary awards, but it cannot make an order that would have the effect of repealing the offending law.

---

<sup>47</sup> Intelligence Services Act 1994, c. 13 (U.K.), available at <http://www.legislation.gov.uk/ukpga/1994/13>.

<sup>48</sup> Regulation of Investigatory Powers Act 2000, c. 23 (U.K.), available at <http://www.legislation.gov.uk/ukpga/2000/23>.

<sup>49</sup> Terrorism Act 2000, c. 11 (U.K.), available at <http://www.legislation.gov.uk/ukpga/2000/11/contents/enacted>.

<sup>50</sup> Anti-Terrorism, Crime and Security Act 2001, c. 24 (U.K.), available at <http://www.legislation.gov.uk/ukpga/2001/24>.

<sup>51</sup> Nigel West, *MI5 as a Model for an American Security Agency*, J. OF HOMELAND SECURITY (Aug. 2006), available at <http://www.homelandsecurity.org/journal/Default.aspx?oid=33&ocat=3>.

<sup>52</sup> Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, 213 U.N.T.S. 222.

<sup>53</sup> Human Rights Act 1998, c. 42 (U.K.), available at <http://www.legislation.gov.uk/ukpga/1998/42>.

<sup>54</sup> See, e.g., *A (FC) and others (FC) v. Sec'y of State for the Home Dep't* [2004] UKHL 56 (U.K.) (The House of Lords found that the indefinite detention of aliens pursuant to the Anti-Terrorism, Crime and Security Act 2001 violated European law, and resulted in the passing of the Prevention of Terrorism Act 2005.).

2011] *CAN WE FIND AND STOP THE “JIHAD JANES”?* 101

Nonetheless, the judgments do often trigger domestic law reforms.<sup>55</sup> For the purposes of this paper, the most important article of the ECHR is Article 8:

- (1) Everyone has the right to respect for his private and family life, his home and his correspondence.
- (2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.<sup>56</sup>

Article 8(2) provides a loophole that can be exploited by the state. As Laura Donohue puts it, “[e]xactly what constitutes a national security concern can be molded to fit the moment.”<sup>57</sup>

### *B. Physical Searches*

In order to obtain a search warrant in criminal cases other than those relating to terrorism, police must satisfy a magistrate “that there are reasonable grounds for believing . . . that an indictable offence [(this is a more serious type of offence, roughly equivalent to a felony)] has been committed . . . and . . . that there is material on [the] premises . . . which is likely to be of substantial value . . . to the investigation of the offence.”<sup>58</sup>

In terrorism cases, police must apply to a magistrate, who may issue a search warrant in relation to specified premises, if “satisfied

---

<sup>55</sup> See, e.g., *Malone v. United Kingdom*, 82 Eur. Ct. H.R. (Ser. B) (1985) (The court found that wiretapping violated Malone’s right to privacy, which led to the enactment of the Interception of Communications Act 1985.). But see Jacqueline Hodgson, *Suspects, Defendants and Victims in the French Criminal Process: The Context of Recent Reform*, 51 INT’L & COMP. L.Q. 781, 782 n.12 (2002) (explaining that France has been condemned by the European Court of Human Rights seventy times between 1981 and 2002 for different human rights violations, including for its treatment of detainees, but has not changed its law significantly).

<sup>56</sup> Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, Nov. 4, 1950, 213 U.N.T.S. 222.

<sup>57</sup> Laura K. Donohue, *Criminal Law: Anglo-American Privacy and Surveillance*, 96 J. CRIM. L. & CRIMINOLOGY, 1059, 1155 (2006).

<sup>58</sup> Police and Criminal Evidence Act 1984, c. 60, § 8 (U.K.), available at <http://www.statutelaw.gov.uk/legResults.aspx?LegType=All+Legislation&searchEnacted=0&extentMatchOnly=0&confersPower=0&blanketAmendment=0&sortAlpha=0&PageNumber=0&NavFrom=0&activeTextDocId=1871554>.

that there are reasonable grounds for suspecting . . . [the presence in those premises of] a person whom the [police officer] reasonably suspects to be<sup>59</sup> . . . or [have] been concerned in the commission, preparation or instigation of acts of terrorism.”<sup>60</sup> If MI5 officers wish to search premises, they need to obtain a warrant from the Secretary of State personally with respect to specified premises. A warrant will be issued if the Secretary of State “thinks it necessary for the action to be taken for the purpose of assisting”<sup>61</sup> the relevant security/intelligence service, and that “the taking of the action is proportionate to what the action seeks to achieve”<sup>62</sup> and that “satisfactory arrangements are in force . . . with respect to the disclosure of information obtained.”<sup>63</sup> A warrant normally expires after six months, but can be renewed for a further period of six months.<sup>64</sup> As Donohue points out, “the device for preventing misuse of [these] powers remains in the control of the Executive – not the Judiciary.”<sup>65</sup> The only “check” on these powers is also non-judicial:

[E]very member of an intelligence service . . . [must] disclose or provide to the Intelligence Services Commissioner all such documents and information as he may require for the purpose of enabling him to carry out his functions . . . [and] after the end of each calendar year, the Intelligence Services Commissioner shall make a report to the Prime Minister . . . [which] [t]he Prime Minister shall lay before each House of Parliament.<sup>66</sup>

### *C. Technological Surveillance*

#### *1. Interception of Communications*

The interception of communications is governed by the Police

---

<sup>59</sup> Terrorism Act 2000, c. 11, § 42(1) (U.K.), available at <http://www.legislation.gov.uk/ukpga/2000/11/contents/enacted>.

<sup>60</sup> *Id.* § 40(1)(b).

<sup>61</sup> Intelligence Services Act 1994, c. 13, § 5(2)(a) (U.K.), available at <http://www.legislation.gov.uk/ukpga/1994/13>.

<sup>62</sup> *Id.* § 5(2)(b).

<sup>63</sup> *Id.* § 5(2)(c).

<sup>64</sup> *Id.* § 6(2)-(3).

<sup>65</sup> DONOHUE, *supra* note 57, at 1159.

<sup>66</sup> Regulation of Investigatory Powers Act 2000, c. 23, § 60(1), (2), (4) (U.K.), available at <http://www.legislation.gov.uk/ukpga/2000/23>.

## 2011] CAN WE FIND AND STOP THE “JIHAD JANES”? 103

Act 1997<sup>67</sup> and Part I of the Regulation of Investigatory Powers Act 2000 (RIPA).<sup>68</sup> Part III of the Police Act 1997 provides an authorization framework for entry onto premises and interference with property or wireless telegraphy.<sup>69</sup> For a warrant to be issued, an authorizing officer has to believe that the authorization is both *necessary* for the action specified to be taken, for the purpose of preventing or detecting serious crime, and that the taking of the action is *proportionate* to what the action seeks to achieve.<sup>70</sup> An offense is defined as a serious crime “if and only if it involves the use of violence, results in substantial financial gain or is conduct by a large number of persons in a common pursuit of a common purpose,” or is the type of offense that would merit a sentence of imprisonment of at least three years for a first time adult offender.<sup>71</sup>

A European court decision confirmed that the sort of interception envisaged by the Police Act did not cover private telephone networks.<sup>72</sup> This decision, together with a European Directive requiring legislation to protect the confidentiality of communications over public networks,<sup>73</sup> triggered the enactment of RIPA.<sup>74</sup>

Part I of RIPA sets out a framework for the lawful interception by security and intelligence services of all communications in the course of transmission by means of the post, or public and private telecommunications systems.<sup>75</sup> As defined in RIPA, “‘communication’ includes . . . anything comprising speech, music, sounds, visual images or data of any description; and . . . signals serving either for the impartation of anything between persons, between a person and a thing or between things or for the actuation or control of any apparatus.”<sup>76</sup>

---

<sup>67</sup> Police Act 1997, c. 50 (Eng.).

<sup>68</sup> Regulation of Investigatory Powers Act 2000, c. 23 (U.K.), available at <http://www.legislation.gov.uk/ukpga/2000/23>.

<sup>69</sup> Police Act 1997, §§ 92-108, c. 50 (Eng.).

<sup>70</sup> *Id.* § 93(2).

<sup>71</sup> *Id.* § 93(4).

<sup>72</sup> Halford v. United Kingdom, App. No. 20605/92, 24 Eur. H.R. Rep. 523 (1997).

<sup>73</sup> Telecom. (Data Protection and Privacy) Regulations, 1999, S.I. 2093 (U.K.), replaced by Privacy and Electronic Communications (EC Directive) Regulations, 2003, S.I. 2426 (U.K.).

<sup>74</sup> VICTORIA WILLIAMS, SURVEILLANCE AND INTELLIGENCE LAW HANDBOOK 67 (Oxford Univ. Press 2006).

<sup>75</sup> Regulation of Investigatory Powers Act 2000, c. 23, §§ 1-25 (U.K.), available at <http://www.legislation.gov.uk/ukpga/2000/23>.

<sup>76</sup> *Id.* § 81(1)(b), (c).

There are some limited situations where interception may be conducted without a warrant, such as where the interception is to obtain information about the communications of someone overseas using a public telecommunications service, and where the provider of that service is required by its domestic law to facilitate the interception.<sup>77</sup> However, warrants for interception and disclosure of information generally must be sought from the Secretary of State.

For a warrant to be issued, the Secretary of State must be satisfied that what the action seeks to achieve is necessary for one or more of the following reasons: it is in the interests of national security; it is for the purpose of preventing or detecting serious crime; it is to safeguard the economic well-being of the United Kingdom (if the information sought relates to acts or intentions outside the British Isles); or to give effect to an international mutual assistance treaty.<sup>78</sup> The conduct authorized by the warrant must also be proportionate to what is sought to be achieved.<sup>79</sup> If the application names one person as the target, it can authorize interception at numerous premises, but must set out which communications are to be intercepted.<sup>80</sup> If a warrant is sought for the interception of communications sent or received outside the British Isles, there is no requirement of proportionality or of naming a subject or premises.<sup>81</sup> RIPA warrants are effective for three months and may be renewed.<sup>82</sup>

There are safeguards similar to the U.S. FISA minimization procedures, discussed below, in that the Secretary of State has a statutory duty to ensure that arrangements are in place for ensuring the disclosure of intercepted material is kept to a minimum, and for destroying it when it is no longer necessary to retain it.<sup>83</sup>

One significant feature of RIPA relates to the inability to use *intercepted* material in most court proceedings. Intercepted material may only be used in court if the material has been

---

<sup>77</sup> *Id.* §§ 3-4.

<sup>78</sup> *Id.* § 5.

<sup>79</sup> WILLIAMS, *supra* note 74, at 74 (discussing Regulation of Investigatory Powers Act 2000, c. 23, § 5 (U.K.)).

<sup>80</sup> *Id.* at 74-75 (discussing Regulation of Investigatory Powers Act 2000, c. 23, § 8 (U.K.)).

<sup>81</sup> *Id.* at 75.

<sup>82</sup> *Id.*

<sup>83</sup> *Id.* at 76 (discussing Regulation of Investigatory Powers Act 2000, c. 23, § 15 (U.K.)).

2011] *CAN WE FIND AND STOP THE “JIHAD JANES”?* 105

lawfully intercepted without a warrant (for example, with the consent of the person who sends the communication),<sup>84</sup> or where it is to be used in certain specified proceedings. Such proceedings include the Proscribed Organizations Appeal Commission or the Special Immigration Appeals Commission (SIAC), which hears cases relating to control orders (orders of house arrest of suspected terrorists) pursuant to the Prevention of Terrorism Act 2005.<sup>85</sup> In SIAC cases the evidence is not disclosed to the defendant or his attorney, but to a Special Advocate acting on his behalf. This clearly causes many difficulties in presenting evidence in prosecutions. This *intercepted* material is to be distinguished from evidence derived from *surveillance*, described below, which may be used in court. The distinction is not always easy to make.<sup>86</sup>

As to oversight, an Interception of Communication Commissioner has been appointed to inquire into and oversee remedies for violation of RIPA. Laura Donohue questions the effectiveness of this process, commenting that the evidence shows few rulings in favor of complainants.<sup>87</sup>

## 2. *Surveillance*

Part II of RIPA sets out authorization procedures for three types of covert surveillance: directed; intrusive; and covert human intelligence. Each of these are described below, and may be conducted not only by the security services, but also by “public bodies”—more than 950 entities<sup>88</sup>—for the purposes of a specific investigation which is likely to reveal private information.<sup>89</sup> RIPA essentially creates a voluntary scheme for authorization, without imposing any form of legal duty upon public authorities to obtain prior authorization. If public authorities fail to follow RIPA procedures, they run the risk of evidence being excluded in any court hearing, or the body being found as having acted in violation of the Human Rights Act 1998.<sup>90</sup> The authorization is an internal

---

<sup>84</sup> Regulation of Investigatory Powers Act 2000, § 3, c. 23 (U.K.).

<sup>85</sup> Prevention of Terrorism Act, 2005, c. 2, §§ 2-4 (Eng.).

<sup>86</sup> *See, e.g., R. v. Hardy and Hardy* [2002] EWCA (Crim) 3012, [2003] 1 Cr. App. R. 30 (U.K.) (prosecution evidence of conversations taped by police was admissible on grounds that it was surveillance as opposed to interception).

<sup>87</sup> LAURA K. DONOHUE, *THE COST OF COUNTERTERRORISM: POWER, POLITICS, AND LIBERTY* 199 (Cambridge Univ. Press 2008).

<sup>88</sup> *Id.* at 202.

<sup>89</sup> Regulation of Investigatory Powers Act 2000, c. 26, § 8 (U.K.).

<sup>90</sup> WILLIAMS, *supra* note 74, at 125-26.

process with post hoc oversight by the Intelligence Services Commissioner for the intelligence services, and by the Surveillance Commissioner for the other public bodies.<sup>91</sup> Both Commissioners are statutorily required to be former senior judges.<sup>92</sup>

Surveillance generally includes monitoring, observing, listening to, and recording persons' conversations, movements, activities and communications with the aid of a surveillance device. Surveillance is covert if it is done in such a way that the persons subject to it are unaware that it is taking place.<sup>93</sup> Duration of surveillance may be only for seventy-two hours in urgent cases, or in cases where applications were made orally. In all other cases, surveillance may only last up to three months, but the permit is renewable.<sup>94</sup> Despite the Home Office declaring that hundreds of lives have been saved by covert surveillance, it says that the techniques need to adapt to changes in technology and the threats the United Kingdom faces.<sup>95</sup>

Directed surveillance<sup>96</sup> focuses on information sought in an investigation where it is expected that private information will be obtained. The Covert Surveillance Code of Practice confirms that this includes information relating to private or family life,<sup>97</sup> so there could be claims that this type of surveillance violates Article 8 of the ECHR. Applications for directed surveillance will be authorized if the authorizing officer believes that the authorization is necessary (on one or more specified grounds, such as being in the interests of national security or for the purpose of preventing or detecting crime<sup>98</sup>) and proportionate. If the information is confidential, a more senior officer has to approve the application.

Intrusive surveillance<sup>99</sup> covers covert searches by persons, or the use of surveillance devices in residential premises or in private vehicles. The tests of necessity and proportionality are required for authorization, but the list of grounds for necessity is far narrower than that required for directed surveillance, comprising

---

<sup>91</sup> *Id.*

<sup>92</sup> Regulation of Investigatory Powers Act 2000, c. 26, § 8 (U.K.).

<sup>93</sup> WILLIAMS, *supra* note 74, at 127 (discussing Regulation of Investigatory Powers Act 2000, § 26(2), (3) & (9), c. 26 (U.K.)).

<sup>94</sup> Regulation of Investigatory Powers Act 2000, c. 26, § 43 (U.K.).

<sup>95</sup> CONTEST, *supra* note 29, at 70-71.

<sup>96</sup> Regulation of Investigatory Powers Act 2000, c. 26, § 26(2) (U.K.).

<sup>97</sup> Covert Surveillance: Code of Practice, 2002, S.I. 1933, § 4.1 (U.K.), *pursuant to* Regulation of Investigatory Powers Act 2000, c. 23, § 71 (U.K.).

<sup>98</sup> Regulation of Investigatory Powers Act 2000, c. 26, § 28(3) (U.K.).

<sup>99</sup> *Id.* § 26(3).

2011] *CAN WE FIND AND STOP THE “JIHAD JANES”?* 107

only three matters: (1) national security; (2) prevention or detection of *serious* crime; and (3) the economic well-being of the United Kingdom. Additionally, it is necessary to show that the evidence cannot be obtained by other means.<sup>100</sup>

The third category, “covert human intelligence sources,” deals with the process by which persons—including public authorities—develop relationships, and then use those relationships covertly to obtain, provide, or disclose information to third parties.<sup>101</sup> Authorization will be granted if the surveillance is necessary and proportionate, and if certain arrangements are in place relating to both the supervision of this surveillance and the way the information is handled.<sup>102</sup> The two Commissioners, as described above, oversee the arrangements. In Laura Donohue’s view, the standard of review is remarkably weak.<sup>103</sup>

Part III of RIPA deals with encrypted data. Parties possessing encryption keys, i.e. codes or passwords allowing general access to electronic data or decoding encrypted electronic data,<sup>104</sup> are obliged to hand them over to the state on the same grounds as are applicable to intrusive surveillance, with the additional ground that it is not reasonably practicable to obtain the information without the encryption key.<sup>105</sup> This part of RIPA only came into force on October 1, 2007, after extensive consultation, which resulted in the publication of a Code of Practice.<sup>106</sup>

### 3. *Transactional Data*

In order to comply with the European Union Data Protection Directive 1995,<sup>107</sup> the United Kingdom enacted the Data Protection Act 1998.<sup>108</sup> This deals, *inter alia*, with how personal data may be processed, disclosed, retained, and for how long, in accordance with the following principles. There must be a legitimate basis for processing relevant information that is not excessive in amount in relation to the purpose for the processing,

---

<sup>100</sup> *Id.* §§ 32(3)-(4).

<sup>101</sup> *Id.* §§ 26(7), (8), (9).

<sup>102</sup> *Id.* § 29.

<sup>103</sup> DONOHUE, *supra* note 87, at 204.

<sup>104</sup> Regulation of Investigatory Powers Act 2000, c. 26, § 56(1) (U.K.).

<sup>105</sup> *Id.* §§ 49-51.

<sup>106</sup> Investigation of Protected Electronic Information: Code of Practice, 2007 (U.K.), *pursuant to* Regulation of Investigatory Powers Act (2000), c. 23 (U.K.).

<sup>107</sup> Council Directive 95/46, 1995 O.J. (L 281) 31 (EC).

<sup>108</sup> Data Protection Act, 1998, c. 29 (U.K.).

and such information should not be held any longer than necessary. As to disclosure, note that information about private life, including correspondence, is protected by Article 8 of the ECHR, save in certain cases, including those of national security or crime prevention.

Under data protection legislation, information was only allowed to be retained by companies for a relatively short time. To address concerns that this might impede collection under RIPA, the Anti-Terrorism, Crime and Security Act 2001 made it a requirement that communication device providers retain data for a specified period.<sup>109</sup> Donohue notes that this information “may relate directly or indirectly to national security” and points out that “may” also suggests “may not”—thus highlighting the potential wide range of data that could fall under the scope of the statute.<sup>110</sup> The statute also prevents HM Revenue and Customs from claiming secrecy to prevent the handing over of financial records and tax information to intelligence services.<sup>111</sup> Donohue queries whether provisions such as these are incompatible with Article 8 of the ECHR.<sup>112</sup> However, Article 15(1) of the ECHR permits the archiving of information in the interest of national security, defense, public security, and for the prevention or detection of criminal offenses.<sup>113</sup>

#### 4. Public Surveillance

There are over four million closed circuit televisions (CCTV) cameras in the United Kingdom, one for every fourteen persons. It is estimated that Britain has “20 per cent of cameras globally and that each person in the country is caught on camera an average of 300 times daily.”<sup>114</sup> It is highly questionable how effective these are to deter crime or catch criminals,<sup>115</sup> or to find potential terrorists.

Although, in principle, the use of CCTV cameras is governed by the principles of the Data Protection Act 1998, until recently

---

<sup>109</sup> Anti-terrorism, Crime and Security Act, 2001, c. 24, §§ 102-04 (U.K.).

<sup>110</sup> DONOHUE, *supra* note 87, at 210-11.

<sup>111</sup> Anti-Terrorism, Crime and Security Act 2001, c. 24, § 19, (U.K.).

<sup>112</sup> DONOHUE, *supra* note 87, at 212.

<sup>113</sup> *Id.* (referring to Council Directive, 2002 O.J. (L 201) 37-47 (EC)).

<sup>114</sup> Tom Kelly, *Revealed: Big Brother Britain has more CCTV Cameras than China*, MAIL ONLINE (Aug. 11, 2009, 8:50 AM), <http://www.dailymail.co.uk/news/article-1205607/Shock-figures-reveal-Britain-CCTV-camera-14-people—China.html>.

<sup>115</sup> CHRISTOPHER SLOBOGIN, PRIVACY AT RISK 84-85 (Univ. of Chicago Press 2007).

2011] CAN WE FIND AND STOP THE “JIHAD JANES”? 109

there was no mechanism for enforcement or accountability.<sup>116</sup> As a result, there have been many complaints about their excessive use and effectiveness. However, a regulator has recently been appointed to oversee the United Kingdom’s cameras, and new guidelines were issued<sup>117</sup> following a review by the National CCTV Strategy, a Home Office appointed body.<sup>118</sup>

In summary, the United Kingdom has a wide range of tools allowing extensive investigation mainly on the grounds of necessity to prevent and detect crime (and terrorism), and proportionality. In some cases the powers are restricted to situations where it is not reasonably practicable or possible to elicit the information in any other way. There is oversight in the investigation process, albeit some of it executive rather than judicial. Despite all the above-mentioned tools, the *Prevent* strategy set out in CONTEST,<sup>119</sup> and the vast amount of work now carried out in the United Kingdom to counter radicalization, it is still difficult to find homegrown terrorists in the first place. To put it another way, the detection tools cannot be deployed until potential terrorists are identified.

### III. THE UNITED STATES

“Homegrown terrorists are not created overnight.”<sup>120</sup>

Surely somebody notices when a family member or neighbor is becoming radicalized? Apparently not in the case of Jihad Jane. Her boyfriend said of her: “She seemed normal to me. She was a good person.”<sup>121</sup> It appears that it was her messages on YouTube and in internet chat rooms that brought her to the attention of the

---

<sup>116</sup> *Id.* (quoting Simon Davies); *Re-engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity*, in TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 152 (Philip E. Agre & Marc Rotenberg eds., 1997).

<sup>117</sup> Christopher Hope, *Home Office to unveil first CCTV regulator to take control of Britain’s army of cameras*, TELEGRAPH (Dec. 15, 2009), <http://www.telegraph.co.uk/news/uknews/law-and-order/6812109/Home-Office-to-unveil-first-CCTV-regulator-to-take-control-of-Britains-army-of-cameras.html>.

<sup>118</sup> HOME OFFICE, NATIONAL CCTV STRATEGY (Oct. 2007) (U.K.), [http://www.bhphousing.co.uk/streetcare2.nsf/Files/LBBA-24/\\$FILE/Home%20Office%20National%20CCTV%20Strategy.pdf](http://www.bhphousing.co.uk/streetcare2.nsf/Files/LBBA-24/$FILE/Home%20Office%20National%20CCTV%20Strategy.pdf).

<sup>119</sup> CONTEST, *supra* note 29, at 82-86.

<sup>120</sup> MAJORITY & MINORITY STAFF OF S. COMM. ON HOMELAND SEC. & GOVERNMENTAL AFFAIRS, *supra* note 13.

<sup>121</sup> Ed Pilkington, *Colleen LaRose: All-American Neighbor or Terrorist Jihad Jane?*, GUARDIAN, Mar. 10, 2010, available at <http://www.guardian.co.uk/world/2010/mar/10/colleen-la-rose-jihad-jane-terrorism-arrest>.

FBI. Nor in the case of Faisal Shahzad. The Times Square bomber gave the impression of being a quiet man who raised his children in Shelton, Connecticut, and told neighbors that he worked on Wall Street.<sup>122</sup>

So without a person doing something that others might categorize as suspicious, such as buying vast quantities of hydrogen peroxide or castor beans, or spouting extreme Islamist or other ideological theories in public or on the internet, and without such activity being picked up by a CCTV camera or being reported to the authorities by a concerned “good citizen,” pointers to questionable conduct can go completely unnoticed. So how can law enforcement find the homegrown terrorists, particularly if there is little suspicious conduct?

#### A. *Human Intelligence*

The importance of human intelligence conducted properly should not be underestimated, as it was thanks to an observant street vendor that attention was drawn to the Times Square bomb.<sup>123</sup> However, human intelligence has its limitations, as a human observer may not have continuous access and will only have limited knowledge of a suspect’s thoughts and intentions, as demonstrated by the boyfriend of Jihad Jane. Also, reporting “suspicious activity” can lead to “considerable prejudice and abuse, both personal and political.”<sup>124</sup>

In January 2002, the Department of Justice announced plans for the Terrorism Information and Prevention System (TIPS). The pilot program would have urged large numbers of U.S. citizens to report anything perceived as unusual or suspicious. There was such opposition to this that Congress shut down the TIPS program.<sup>125</sup> Nonetheless, many neighborhood watch schemes operate with little evidence that they have a real impact on finding terrorists and preventing terrorism.<sup>126</sup>

---

<sup>122</sup> *Faisal Shahzad Kept Low Profile in U.S.*, CBS NEWS (May 4, 2010), [www.cbsnews.com/stories/2010/05/04/national/main6459360.shtml](http://www.cbsnews.com/stories/2010/05/04/national/main6459360.shtml).

<sup>123</sup> Al Baker & William K. Rashbaum, *Police Find Car Bomb in Times Square*, N.Y. TIMES, (May 1, 2010), available at [www.nytimes.com/2010/05/02/nyregion/02timesquare.html](http://www.nytimes.com/2010/05/02/nyregion/02timesquare.html).

<sup>124</sup> DONOHUE, *supra* note 87, at 253.

<sup>125</sup> *Id.* at 252.

<sup>126</sup> *Id.* at 254.

2011] CAN WE FIND AND STOP THE “JIHAD JANES”? 111

### B. Technological Surveillance

“Trying to glean actionable intelligence from the flood of information we receive is akin to taking a sip of water from a fire hose.”<sup>127</sup>

Law enforcement authorities have a wide array of tools at their disposal to enable them to collect an enormous amount of intelligence. At one end of the spectrum, there is highly regulated surveillance of U.S. citizens involved in domestic crime, and at the other end, there are the unregulated tools of CCTV cameras in public places and data mining. The legal backdrop is the Fourth Amendment:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the person or things to be seized.<sup>128</sup>

#### 1. Domestic Surveillance

In 1967, a landmark Supreme Court case, *Katz v. United States*,<sup>129</sup> set the baseline where people could expect to be free from “unreasonable searches.” Justice Stewart made it clear that the Fourth Amendment “protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.”<sup>130</sup> As will be seen below, these words have a profound impact in different ways on various sorts of surveillance. *Katz* held that the Fourth Amendment’s requirement for a warrant applied to the conducting of electronic surveillance.<sup>131</sup>

A pen register may be used to trace telephone numbers that have been dialed from a particular land line telephone,<sup>132</sup> but this does not give law enforcement the right to listen to the content of

---

<sup>127</sup> Mueller 2010 Statement, *supra* note 1.

<sup>128</sup> U.S. CONST. amend. IV.

<sup>129</sup> *Katz v. United States*, 389 U.S. 347 (1967).

<sup>130</sup> *Id.* at 351 (citation omitted).

<sup>131</sup> *Id.* at 355-58.

<sup>132</sup> 18 U.S.C. §§ 3121-27 (2000 & Supp. 2003).

the call.<sup>133</sup> The USA PATRIOT Act extended this statutory right to accessing email, ISP and URL addresses.<sup>134</sup> A warrant is required to do this, based on a showing of probable cause that the use of this device is “relevant to an ongoing investigation.”<sup>135</sup> The lower level of probable cause reflects a perception that this type of surveillance amounts to a lower level of intrusion on privacy. Once a potential homegrown terrorist has been identified, it is likely that this sort of surveillance could be used without too much difficulty.

*Katz* was the trigger for Congress to pass the Omnibus Crime Control and Safe Streets Act of 1968.<sup>136</sup> Title III of that Act governs the use of wiretaps for domestic criminal law investigations.<sup>137</sup> An application has to be made for a warrant to conduct electronic surveillance or to obtain access to stored communications, such as email.<sup>138</sup> The statute sets out a detailed list of information that has to be supplied about, *inter alia*, the alleged criminal offense, the identity of the target if known, and a description of other investigative methods used or that could not be used to date.<sup>139</sup> A court will only grant the application for the warrant if it finds probable cause that an offense has been, is being, or is about to be committed.<sup>140</sup> A possible problem caused by the scope of probable cause is discussed below in Part III.

The case commonly referred to as *Keith*<sup>141</sup> took matters further. It concerned whether the President of the United States had the power, acting through the Attorney General, to authorize electronic surveillance in internal security matters without a warrant.<sup>142</sup> The case confirmed that a warrant is required for domestic security surveillance, but did not address the issues that may be involved “with respect to activities of foreign powers or

---

<sup>133</sup> *Smith v. Maryland*, 442 U.S. 735, 741 (1979).

<sup>134</sup> Uniting and Strengthening America by Proving Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, § 216, 115 Stat. 272, 288-91 (2001) [hereinafter USA PATRIOT ACT] (codified as amended at 18 U.S.C. §§ 3121-27 (2000 & Supp. 2003)).

<sup>135</sup> 18 U.S.C. § 3123(a) (2001).

<sup>136</sup> Pub. L. No. 90-351, 82 Stat. 197 (codified as amended at 18 U.S.C. §§ 2510-20 (2000)).

<sup>137</sup> *Id.* at tit. III, 82 Stat. 211.

<sup>138</sup> *Id.*

<sup>139</sup> 18 U.S.C. §§ 2518 (1)(b)-(d), 2703(a) (2000 & Supp. III 2003).

<sup>140</sup> *Id.* § 2518(3)(b).

<sup>141</sup> *United States v. U.S. Dist. Court for the E. Dist. of Mich.*, 407 U.S. 297 (1972).

<sup>142</sup> *Id.* at 299.

2011] *CAN WE FIND AND STOP THE “JIHAD JANES”?* 113

their agents.”<sup>143</sup> Justice Powell went on to recognize that “domestic security surveillance may involve different policy and practical considerations from the surveillance of “ordinary crime. . . . Often too, the emphasis of domestic intelligence gathering is on the prevention of unlawful activity or the enhancement of the Government’s preparedness for some possible future crisis or emergency.”<sup>144</sup>

## 2. *Foreign Surveillance*

If the homegrown terrorist suspect has links and communication with persons overseas, law enforcement authorities have an easier task than when the communications are wholly domestic and Title III procedures have to be followed. The current law is set out in the Foreign Intelligence Surveillance Act of 1978 (FISA),<sup>145</sup> the USA PATRIOT Act of 2001,<sup>146</sup> the Intelligence Reform and Terrorism Prevention Act of 2004,<sup>147</sup> and the FISA Amendments Act of 2008 (FAA).<sup>148</sup> I will discuss certain aspects of the law relevant to potential homegrown terrorists.

FISA and the statutes amending it govern the electronic surveillance of persons in the United States for the purpose of collecting foreign intelligence. Under the USA PATRIOT Act, in order to obtain a FISA warrant, the government has to show that a “significant purpose” of the surveillance is to obtain foreign intelligence.<sup>149</sup> This has been described as a “programmatic purpose, to protect the nation against terrorists and espionage threats directed by foreign powers,” and from FISA’s outset, this purpose has been “distinguishable from ‘ordinary crime control.’”<sup>150</sup> Orders are sought in a special court, the Foreign Intelligence Surveillance Court (FISC), which meets in secret. Under the FAA, U.S. citizens may not be intentionally targeted,<sup>151</sup> but some intercepted communications will necessarily be to or from U.S.

---

<sup>143</sup> *Id.* at 322.

<sup>144</sup> *Id.*

<sup>145</sup> Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended at 50 U.S.C. §§ 1801-11 (2000)).

<sup>146</sup> USA PATRIOT ACT, *supra* note 134.

<sup>147</sup> Pub. L. No. 108-458, 118 Stat. 3638 (2005).

<sup>148</sup> Pub. L. No. 110-261, 122 Stat. 2436 (2008).

<sup>149</sup> 50 U.S.C. § 1804(a)(6)(B) (2010).

<sup>150</sup> *In re: Sealed Case No 02-001, 02-002*, 310 F.3d 717, 746 (FISA Ct. Rev. 2002).

<sup>151</sup> Pub. L. No. 110-261, § 702(b)(1)-(3), 122 Stat. 2438 (2008).

citizens. “The FAA eliminates any showing of individualized suspicion, even where communications of Americans are the foreseeable consequence of FISC orders.”<sup>152</sup>

Under FISA, a “U.S. person,” who is defined as a citizen or permanent resident,<sup>153</sup> may be subject to electronic surveillance<sup>154</sup> on a warrant based on a finding of probable cause that the target of the surveillance is a member of a foreign terrorist group or an agent of a foreign power. However, if the “U.S. person” is merely exercising a First Amendment right of freedom of speech, and there are no other factors in his or her conduct (including past activities) to justify surveillance, then such person cannot be considered to be an agent of a foreign power.<sup>155</sup>

A foreign power includes a group involved in international terrorism.<sup>156</sup> An agent of a foreign power can be someone residing on U.S. soil with a work or visitor’s visa, who engages in preparation for or actual commission of acts of international terrorism.<sup>157</sup> Thus in the original FISA, a “non-U.S. person” could be someone acting alone, without having to show connections to a “foreign power.”<sup>158</sup> Such a person is referred to as a “lone wolf.”<sup>159</sup>

If the warrant targets a “U.S. person,” there must also be probable cause that such person *knowingly* engaged in activities on behalf of a foreign power, which may involve a violation of U.S. criminal law, or *knowingly* engages in preparation for or actual acts of sabotage or international terrorism.<sup>160</sup> The FAA has now removed the requirement that a target be an agent of a foreign power,<sup>161</sup> so now any person in the United States can be a “lone wolf.” However, the lone wolf provisions were due to sunset at the end of 2009, and are currently in the process of being reauthorized.

---

<sup>152</sup> William C. Banks, *Ten Questions: Responses to the ten Questions*, 35 WM. MITCHELL L. REV. 5007, 5014 (2009) (in response to question 9: Is the FISA Amendments Act of 2008 good policy? Is it constitutional?).

<sup>153</sup> 50 U.S.C. § 1801(i) (2010).

<sup>154</sup> “Electronic surveillance” is defined in terms of four categories. *Id.* § 1801(f).

<sup>155</sup> *See id.* § 1805(a).

<sup>156</sup> *Id.*

<sup>157</sup> *Id.* § 1801(b).

<sup>158</sup> *Id.* § 1801(b)(2)(C).

<sup>159</sup> Intelligence Reform and Terrorism Provision Act of 2004, Pub. L. 108-458, § 6001, 118 Stat. at 3638 (2004).

<sup>160</sup> 50 U.S.C. § 1801(b)(2).

<sup>161</sup> *See* Pub. L. No. 110-261, § 702(d)(1), 122 Stat. at 2439 (2008).

## 2011] CAN WE FIND AND STOP THE “JIHAD JANES”? 115

FISA, in its original incarnation, was concerned with the acquisition, rather than the uses that the government might have for the information that is collected. It required that the targets and facilities to where the surveillance would be directed must be known and identified (i.e. it adopted a “person-focused approach”).<sup>162</sup>

Technological changes, where intelligence gathering is now more data-focused, with a central role for the internet and the nature of surveillance in “packet-switched networks,” resulted in the passing of the Protect America Act of 2007.<sup>163</sup> That Act permitted “warrantless surveillance of foreign-to-foreign communications that happened to be routed through the U.S. (considered non-controversial), as well as warrantless surveillance of U.S. citizens communicating with people overseas, as long as the target was reasonably believed to be located outside the U.S.”<sup>164</sup> The impact of this is that the location of the surveillance “no longer correlates to the location of the individuals surveilled.”<sup>165</sup> Now there is also no need for a judicial determination concerning the identity and location of a specific target. Instead, there need only be a determination that a process of surveillance is able to target persons reasonably believed to be located outside the United States to acquire foreign intelligence information.<sup>166</sup> This provision, which has been replicated in the FAA (which replaced the expired PAA), effectively legitimized President Bush’s warrantless Terrorist Surveillance Program (TSP) of Americans inside the United States. Nevertheless, despite this apparent legitimization, a recent United States District Court decision held that the NSA had violated FISA by tapping telephones without a warrant.<sup>167</sup>

The difference between the provisions in the FAA and the TSP is that, instead of specifically targeting people inside the

---

<sup>162</sup> Orin S. Kerr, *Surveillance: Updating the Foreign Intelligence Surveillance Act*, 75 U. CHI. L. REV. 225, 226 (Winter 2008).

<sup>163</sup> *Id.* at 233; Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552 (2007).

<sup>164</sup> Stephanie Cooper Blum, *What Really is at Stake with the FISA Amendments Act of 2008 and Ideas for Future Surveillance Reform*, 18 B.U. PUB. INT. L. J. 269, 295-96 (2009).

<sup>165</sup> Kerr, *supra* note 162, at 234.

<sup>166</sup> Paul M. Schwartz, *Warrantless Wiretapping, FISA Reform, and the Lessons of Public Liberty: A Comment on Holmes’s Jorde Lecture*, 97 CAL. L. REV. 407, 420 (2009).

<sup>167</sup> *In re Nat’l Sec. Agency Telecomm. Records Litig.*, 700 F. Supp.2d 1182 (N.D. Cal. 2010); Daphne Eviatar, *Court Ruling Highlights Need for New State Secrets Law*, HUMAN RIGHTS FIRST BLOG (Apr. 2, 2010, 1:59 PM), <http://blog.humanrightsfirst.org/2010/04/court-ruling-highlights-need-for-new.html>.

United States (as in the TSP), the PAA, and now the FAA, focuses on the location of the target and not his or her status in relation to a foreign power or terrorist organization.<sup>168</sup> According to David Kris, the focus on the location of a target still presents a problem, but he thinks that for now, this may be the best the government can do.<sup>169</sup> He also thinks a solution is still to be found for the problem that the impact of continually changing technology has on ensuring that email communications fall within FISA.<sup>170</sup> Another concern is that the breadth of the FAA means that it is performing “vacuum cleaner” surveillance and data mining.<sup>171</sup>

Generally, in the case of “U.S. persons,” there have to be minimization procedures in place to ensure that the material collected during surveillance will not be disseminated or retained outside defined boundaries, and the FAA has extended these, although information such as a “U.S. person’s” identity that is “necessary to understand foreign intelligence information” or is needed to assess its importance, can be retained.<sup>172</sup> The FAA has given the government “a vastly expanded reservoir of foreign-to-domestic communications from which it can cull information about non-targeted U.S. persons.”<sup>173</sup> There are also still concerns that a large number of incidental communications by innocent Americans can now be acquired without a warrant.<sup>174</sup> For example, currently a group of lawyers, human rights activists, and journalists are arguing that the FAA has had an adverse impact on their freedom to do normal day-to-day work, which may include communicating with former detainees of the CIA’s rendition and detention programs. However, these plaintiffs are encountering problems of standing (i.e. being able to prove that they personally have been subject to surveillance).<sup>175</sup>

---

<sup>168</sup> Banks, *supra* note 152, at 5013 (in answer to question 9: Is the FISA Amendments Act of 2008 good policy? Is it constitutional?).

<sup>169</sup> David S. Kris, *Modernizing the Foreign Intelligence Surveillance Act: Progress to Date and Work Still to Come*, in LEGISLATING THE WAR ON TERROR: AN AGENDA FOR REFORM 217, 237 (2009).

<sup>170</sup> *Id.* at 234-35.

<sup>171</sup> Banks, *supra* note 152, at 5014 (in answer to question 9: Is the FISA Amendments Act of 2008 good policy? Is it constitutional?).

<sup>172</sup> 50 U.S.C. § 1801(h)(2) (2006).

<sup>173</sup> Martin Lederman, *The Key Questions About the New FISA Bill*, BALKINIZATION BLOG (June 22, 2008, 8:27 PM), <http://balkin.blogspot.com/2008/06/key-questions-about-new-fisa-bill.html>.

<sup>174</sup> Cooper Blum, *supra* note 164, at 302.

<sup>175</sup> *Amnesty Int’l v. Blair*, No. 09-4112-CV (2d Cir.), *sub nom.* *Amnesty Int’l USA v. McConnell*, 646 F. Supp.2d 633 (S.D.N.Y. 2009); Ellen Nakashima, *For group, surveillance*

## 2011] CAN WE FIND AND STOP THE “JIHAD JANES”? 117

By way of completeness, FISA was amended to permit the use of pen registers and trap and trace devices<sup>176</sup> to track instruments from which wire or electronic communications are transmitted, as well as email and web page addresses. Instead of having to satisfy the usual FISA probable cause requirement, the applicant merely has to certify that the “information likely to be obtained is foreign intelligence information not concerning a United States person or is relevant to an ongoing investigation to protect against international terrorism,” provided that such investigation of a “U.S. person” is not based solely on activities protected by the First Amendment.<sup>177</sup> Cell phones can also now be tapped.<sup>178</sup> The Director of National Intelligence and the Attorney General are allowed to issue directives to persons—a term that includes agents of communications service providers—delineating the assistance needed to acquire foreign intelligence information.<sup>179</sup> The constitutionality of this practice was confirmed by the FISCR in 2008.<sup>180</sup>

Having said all of this, it is still a fact that “the government can’t get a FISA warrant just to find out whether someone is a terrorist: it has to already believe he is one.”<sup>181</sup> Some commentators believe that FISA does not work when there is an urgent need for “detection before an act of terrorism ha[s] been detected.”<sup>182</sup> Shane Harris puts it another way:

The intelligence agencies [have not] been able to move beyond ‘guilt by association’ as the best indicator of whether someone was, or wasn’t a terrorist. . . . Our current surveillance laws are engineered to allow the intelligence community to consume huge amounts of data, in the hopes that some of it will prove useful. Again we see that the Watchers have become very good at collecting dots but not at connecting them.”<sup>183</sup>

---

*law is elusive legal target*, WASH. POST, Apr. 19, 2010, at A6.

<sup>176</sup> 50 U.S.C. §§ 1841-46 (2000 & Supp. III 2003).

<sup>177</sup> USA PATRIOT ACT, *supra* note 134, § 214(a)(2), 115 Stat. 286.

<sup>178</sup> *Id.* § 206.

<sup>179</sup> 50 U.S.C. § 1805(b) (2006), *repealed by* Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. No. 110-261, § 403(a)(1)(A), 122 Stat. 2436, 2473 (2008).

<sup>180</sup> *In re* Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d. 1004 (FISA Ct. Rev. 2008).

<sup>181</sup> Cooper Blum, *supra* note 164, at 293 (quoting RICHARD POSNER, NOT A SUICIDE PACT: THE CONSTITUTION IN A TIME OF NATIONAL EMERGENCY 94 (2006)).

<sup>182</sup> GABRIEL SCHOENFELD, NECESSARY SECRETS: NATIONAL SECURITY, THE MEDIA, AND THE RULE OF LAW 38 (2010).

<sup>183</sup> SHANE HARRIS, THE WATCHERS 360-61 (2010).

### 3. *Transactional Information*

Another tool that can yield information about a potential homegrown terrorist is the collection of transactional data (i.e. records from banks, telephone companies, internet service providers, credit agencies and travel agencies). Let us not overlook the fact that private industry has extensive access to personal information about most Americans. Some of these companies, such as SeisInt (owned by LexisNexis) and ChoicePoint provide enormous quantities of personal information, including medical records, property deeds, and court filings to government agencies.<sup>184</sup> The legal basis for this comes from the line of cases that includes *Smith v. Maryland*,<sup>185</sup> where Justice Blackmun said: “This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.”

Transaction surveillance never requires probable cause or reasonable suspicion, even when its primary purpose is a criminal investigation. The government can seek transactional information with a subpoena, which is easily obtained on a showing that the information sought is relevant to a legitimate (statutorily authorized) investigation.<sup>186</sup>

One form of administrative subpoena is a national security letter (NSL).<sup>187</sup> For this to be issued, it must be “relevant to any authorized investigation to protect against international terrorism or clandestine intelligence activities.”<sup>188</sup> One significant feature of the NSL was that the statute placed an “indefinite gag” on anyone served with it.<sup>189</sup> After the scheme was declared unconstitutional to the extent that it immunized NSLs from judicial process and third-party record holders could not challenge them,<sup>190</sup> the statute was amended to permit third parties to ask a court to set NSLs aside when they are “unreasonable, oppressive or otherwise unlawful, as well as challenge any accompanying gag order.”<sup>191</sup>

---

<sup>184</sup> SLOBOGIN, *supra* note 115, at 10.

<sup>185</sup> *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979).

<sup>186</sup> SLOBOGIN, *supra* note 115, at 170.

<sup>187</sup> USA PATRIOT ACT, *supra* note 134, § 210 (codified as amended at 18 U.S.C. § 2703(c)(2)) (2000 & Supp. I 2001).

<sup>188</sup> 18 U.S.C. § 2709(b)(1) (2006).

<sup>189</sup> DONOHUE, *supra* note 87, at 236.

<sup>190</sup> *Doe v. Ashcroft*, 334 F. Supp.2d 471 (S.D.N.Y. 2004); *Doe v. Gonzales*, 386 F. Supp.2d 66 (D. Conn. 2005).

<sup>191</sup> *See, e.g.*, 18 U.S.C. § 3511(a)-(b) (2006).

2011] *CAN WE FIND AND STOP THE “JIHAD JANES”?* 119

Slobogin describes this judicial review power as “relatively toothless,”<sup>192</sup> as the court in *Doe v. Ashcroft* said that the standard of review for NSLs was “so minimal that most such NSLs would likely be upheld in court.”<sup>193</sup> Laura Donohue comments that despite the statutory amendments, the power to collect massive amounts of information has few regulations. Minimal restrictions are placed on who sees the information, how long it is kept and what purpose the information is used for.<sup>194</sup> Some commentators complain about the lack of restrictions and offer suggestions for regulation.<sup>195</sup> Other commentators think that it is unlikely that the law will move towards protecting privacy when “fear of terrorism drives the political agenda.”<sup>196</sup>

In early 2010, the NSL process attracted bad press because it had not followed its own minimal procedures to obtain information,<sup>197</sup> and this was confirmed by a Department of Justice Report.<sup>198</sup> In any event, law enforcement officers can easily obtain access to plenty of transactional information about any suspected homegrown terrorist, provided that such a person is identified in the first place.

#### 4. *Public Surveillance*

A survey of the tools available to find potential homegrown terrorists is not complete without reference to public surveillance. *Kyllo v. United States*<sup>199</sup> concerned whether the warrantless use of a thermal-imaging device in the street that discovered marijuana growing inside Kyllo’s home, violated the Fourth Amendment. It

---

<sup>192</sup> SLOBOGIN, *supra* note 115, at 178.

<sup>193</sup> See *Ashcroft*, 334 F. Supp.2d at 502.

<sup>194</sup> DONOHUE, *supra* note 87, at 243.

<sup>195</sup> See, e.g., SLOBOGIN, *supra* note 115 (a complicated proposal of applying a sliding scale of relevance, reasonable suspicion and probable cause before obtaining these records); Orin Kerr, *2009 Survey of Books Related to the Law: Review: Do We Need A New Fourth Amendment?*, 107 MICH. L. REV. 951 (2009) (a balancing test to evaluate the public interest in investigative needs against the public interest in privacy in contemporary technology).

<sup>196</sup> WHITFIELD DIFFIE & SUSAN LANDAU, *PRIVACY ON THE LINE: THE POLITICS OF WIRETAPPING AND ENCRYPTION* 155 (2007).

<sup>197</sup> John Solomon & Carrie Johnson, *FBI broke the law for years in phone record searches*, WASH. POST. (Jan. 19, 2010), available at <http://www.washingtonpost.com/wp-dyn/content/article/2010/01/18/AR2010011803982.html>.

<sup>198</sup> U.S. DEPT. OF JUSTICE, OFFICE OF THE INSPECTOR GEN., *A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION’S USE OF EXIGENT LETTERS AND OTHER INFORMAL REQUESTS FOR TELEPHONE RECORDS* (2010).

<sup>199</sup> *Kyllo v. United States*, 533 U.S. 27 (2001).

was held that where “the Government uses a device that is not in general public use, to explore details of a home that would previously have been unknowable without physical intrusion, that surveillance is a “search” and is presumptively unreasonable without a warrant.”<sup>200</sup> As technology advances and viewing enhancement devices become more readily available, this may well affect what is classified a Fourth Amendment protected search.<sup>201</sup>

*United States v. Knotts*<sup>202</sup> concerned whether the use of an electronic beeper to track the movement of a car violated the Fourth Amendment. The Court held that a person in a car on a public road has no reasonable expectation of privacy, whether spotted by a beeper or the naked eye. The court did comment that Knott’s observation that beeper tracking might constitute twenty-four hour surveillance of any citizen, without judicial notice or supervision, i.e. a “dragnet” practice, might raise constitutional issues.<sup>203</sup> Slobogin refers to *Knotts*, and the fact that full-time surveillance of the public is the norm in many places, to make his argument that the Fourth Amendment should recognize a public right of anonymity.<sup>204</sup> Donohue thinks that there are legitimate law enforcement interests in this type of surveillance to prevent and detect crime,<sup>205</sup> but she and others point to the fact that no jurisdiction is keeping the sort of data that can be analyzed to assess the effect of the cameras on any crime,<sup>206</sup> let alone in finding a potential homegrown terrorist.

Finally on the subject of public surveillance, I turn briefly to the subject of random suspicionless searches, such as that carried out on the riders of the New York subway.<sup>207</sup> The constitutionality of this particular search was upheld,<sup>208</sup> but I mention it only to highlight that police would be very lucky to spot a homegrown or

---

<sup>200</sup> *Id.* at 40.

<sup>201</sup> SLOBOGIN, *supra* note 115, at 52-81.

<sup>202</sup> *United States v. Knotts*, 460 U.S. 276 (1983).

<sup>203</sup> *Id.* at 284.

<sup>204</sup> SLOBOGIN, *supra* note 115, at 79-81.

<sup>205</sup> DONOHUE, *supra* note 87, at 218; Sharon Bradford Franklin, *Watching the Watchers: Establishing Limits on Public Video Surveillance*, 32 CHAMPION 40, 40-41 (Apr. 2008), <http://www.constitutionproject.org/pdf/WatchingWatchers.pdf>.

<sup>206</sup> DONOHUE, *supra* note 87, at 218 (quoting *Privacy vs. Security: Electronic Surveillance in the Nation’s Capital: Hearing Before the Subcomm. of the D.C. of the Comm. On Government Reform*, 107th Cong. 2 (2002)).

<sup>207</sup> See, e.g., Al Baker, *Subway Searches Go on Quietly, Just How Police Like Them*, N.Y. TIMES, (July 6, 2007), <http://www.nytimes.com/2007/07/06/nyregion/06bags.html>.

<sup>208</sup> *MacWade v. Kelly*, 460 F.3d 260 (2d Cir. 2006).

2011] *CAN WE FIND AND STOP THE "JIHAD JANES"?* 121

any terrorist in a random search.

#### IV. A GAP IN THE ARMORY?

If law enforcement personnel believe that their homegrown suspect is communicating with other "U.S. persons," and they want to conduct surveillance on that suspect, but they do not know exactly what offense is planned and they do not know whether some unspecified offense is being committed or about to be committed,<sup>209</sup> they will not be able to establish the probable cause to obtain the warrant. What does "probable cause" mean? What does "about to be committed" mean? How close to the actual stage of commission does this have to be?

I suggest that the above words in 18 U.S.C.A. § 2518(3)(a) expose a gap in the array of tools available to detect potential terrorists and investigate potential terrorist crimes so that they can be forestalled. Justice Powell envisaged this sort of problem in *United States v. United States District Court for the Eastern District of Michigan*:

Given th[e] potential distinctions between Title III criminal surveillances and those involving the domestic security, Congress may wish to consider protective standards for the latter which differ from those already prescribed for specified crimes in Title III.<sup>210</sup>

Further, the court suggested that "a domestic security surveillance statute could deviate from Title III in at least three ways: (1) "the application and affidavit showing probable cause need not follow the exact requirements of 18 U.S.C. § 2518 but should allege other circumstances more appropriate to domestic security cases"; (2) "the request for prior court authorization could, in sensitive cases, be made to any member of a specially designated court"; and (3) "the time and reporting requirements need not be so strict as those in 18 U.S.C. § 2518."<sup>211</sup> To date Congress has not legislated to deal with this problem. With the advent of the homegrown terrorist, perhaps now is the time.

What does probable cause mean? The phrase embodies a "practical nontechnical conception" but one that necessarily relates to a suspicion that a particular person has committed a

---

<sup>209</sup> 18 U.S.C.A. § 2518(3)(a) (1998).

<sup>210</sup> *United States v. U.S. Dist. Court for the E. Dist. of Mich.*, 407 U.S. 297, 322 (1972).

<sup>211</sup> DAVID S. KRIS, *NATIONAL SECURITY INVESTIGATIONS*, § 11.13 (Thomson/West, 2007) (quoting *U.S. Dist. Court for the E. Dist. of Mich.*, 407 U.S. at 323).

crime.<sup>212</sup> And yet the standard seems to fluctuate, either in terms of percentage values that have been cited to explain it,<sup>213</sup> or because of the evolution of the reasonable suspicion standard into Fourth Amendment jurisprudence.<sup>214</sup>

In *United States v. Knights*, Chief Justice Rehnquist said “[a]lthough the Fourth Amendment ordinarily requires the degree of probability embodied in the term ‘probable cause,’ a lesser degree satisfies the Constitution when the balance of governmental and private interests makes such a standard reasonable.”<sup>215</sup> According to Chief Justice Rehnquist, the reasonable suspicion analysis is applied rather than that of probable cause, “when it is ‘reasonable.’”<sup>216</sup> He did not continue to suggest when it might be appropriate to do so.

The lower standard is often applied in “special needs” situations, “beyond the normal need for law enforcement,”<sup>217</sup> such as in stops at airports<sup>218</sup> or checkpoints.<sup>219</sup> It is important to have the facility of “special needs” because “an inflexible probable cause requirement proves impossible to maintain because it limits the police’s ability to stop suspicious behavior from blossoming into dangerous criminal activity.”<sup>220</sup> Orin Kerr suggests that *Keith* was “an early application of the Fourth Amendment’s ‘special needs’ doctrine, but whereas *Keith* focused on identity, modern ‘special needs’ cases focus on the ‘programmatically purpose’ of governmental conduct.”<sup>221</sup> I suggest that issuing a warrant to search the premises of a potential terrorist based on a finding of

---

<sup>212</sup> *Illinois v. Gates*, 462 U.S. 213, 231 (1983) (quoting *Brinegar v. United States*, 338 U.S. 160, 176 (1949)).

<sup>213</sup> See, e.g., Craig S. Lerner, *The Reasonableness of Probable Cause*, 81 TEX. L. REV. 951 (2003) (discussing FBI counsel’s comment that when she wanted to obtain a FISA warrant to search the computer of Zacarias Moussaoui, she placed the likelihood that he was an agent of a foreign power as greater than fifty percent, but her local U.S. Attorney’s office were regularly requiring seventy five to eight percent probability, and sometimes even higher); SLOBOGIN, *supra* note 115, at 38 (“Probable cause is often equated with a more-likely-than-not (51 percent) finding or perhaps a level of certainty somewhat below that.”).

<sup>214</sup> See, e.g., Lerner, *supra* note 213; Kit Kinports, *Diminishing Probable Cause and Minimalist Searches*, 6 OHIO ST. J. CRIM. L. 649 (2009).

<sup>215</sup> *United States v. Knights*, 534 U.S. 112, 121 (2001).

<sup>216</sup> Lerner, *supra* note 213, at 1003.

<sup>217</sup> *New Jersey v. T.L.O.*, 469 U.S. 325, 351 (1985).

<sup>218</sup> *United States v. Moreno*, 475 F.2d 44, 45 (5th Cir. 1973).

<sup>219</sup> *Mich. Dep’t. of State Police v. Sitz*, 496 U.S. 444, 455 (1990).

<sup>220</sup> Ricardo J. Bascuas, *Fourth Amendment Lessons from the Highway and the Subway: A Principled Approach to Suspicionless Searches*, 38 RUTGERS L.J. 719, 745 (2007).

<sup>221</sup> Kerr, *supra* note 162, at 226.

2011] *CAN WE FIND AND STOP THE “JIHAD JANES”?* 123

reasonable suspicion might be in the category of circumstances envisaged by Chief Justice Rehnquist referred to above.

Another approach would be for Congress to amend terrorist offenses to include preparatory, planning or threatening conduct. If probable cause remains the standard to satisfy before a warrant may be issued, then lowering the threshold to include acts further back in the chain of commission, such as preparation and instigation, may assist law enforcement authorities in detection and prevention, although not necessarily in making the original identification of a potential terrorist.

## V. CONCLUSION

“For all the money spent, the hours consumed, for all the programs run in secret and at extraordinary political and social cost, the government was not much better at detecting bad guys than they were on 9/11.”<sup>222</sup>

The United Kingdom and the United States approach the problem of finding and stopping homegrown terrorists such as Jihad Jane in broadly similar ways, but the methods differ in several significant respects. In the broadest sense, both countries use the tools of physical searches and surveillance, and electronic surveillance.

In the United States, not only are U.S. citizens and permanent residents treated differently from others residing or present on home soil, but also domestic and foreign surveillance are treated differently. It is far harder to obtain a warrant if communications are between persons in the United States than if there is a foreign element introduced. It is harder to make a showing of probable cause that a crime has been, is, or is about to be committed, than one of probable cause that a “U.S. person” *knowingly* engaged in activities on behalf of a foreign power, which may involve a violation of U.S. criminal law, or *knowingly* engages in preparation for or in actual acts of sabotage or international terrorism,<sup>223</sup> as the FISA requirement can cover acts further back in the chain of commission.

In the United Kingdom, residents and aliens are treated alike, and there is one body of legislation to deal with domestic and

---

<sup>222</sup> HARRIS, *supra* note 183, at 360.

<sup>223</sup> 50 U.S.C.A. § 1801(b)(2) (2008).

foreign surveillance. The highest standard that is required before a warrant may be issued is reasonable suspicion or reasonable belief. Some commentators say that this standard has been equated with a thirty percent level of certainty.<sup>224</sup> The RIPA warrants are issued on showings of necessity and proportionality. Thus, it would appear that warrants are easier to obtain in the United Kingdom than in the United States.

The highest amount of judicial oversight is seen in the application for Title III warrants in the United States and for some search warrants in the United Kingdom. FISA warrants are issued by a secret court, and RIPA warrants are administrative, not judicial, although there is oversight by Commissioners who are retired judges.

David Kris has suggested that national security investigations in the United States could be simplified by having two major collection statutes: one dealing with acquisition of information where warrants are required on a showing of probable cause; and the other dealing with the sort of surveillance conducted by pen registers and trap and trace devices, and yielding transactional data by means of national security letters.<sup>225</sup>

Times have changed since *Keith* was decided. In 1973, as well as during the years that have followed, the attitude was that “the needs of the executive are so compelling in the area of foreign intelligence, unlike the area of domestic security.”<sup>226</sup> The United Kingdom has had homegrown terrorists for years, and treats them the same as “international” terrorists. Recent events in the United States surely demonstrate that the needs of the executive in the area of domestic security are becoming equivalent to the needs where foreign intelligence is involved—not least because the increased use of the internet by terrorists has blurred the distinction between what is domestic-based and what is foreign-based terrorism. U.K. law is not perfect by any means, but perhaps a model which recognizes that citizens may present as grave a threat as aliens, with no difference between domestic and foreign intelligence surveillance techniques, would be more appropriate for dealing with current needs to counter terrorist

---

<sup>224</sup> SLOBOGIN, *supra* note 115, at 38 (referring to C.M.A. McCauliff, *Burdens of Proof: Degrees of Belief. Quanta of Evidence, or Constitutional Guarantees*, 35 VAND. L. REV. 1293, 1325 (1982) (summarizing a survey of federal judges)).

<sup>225</sup> Kris, *supra* note 169, at 234-35.

<sup>226</sup> *United States v. Truong Dinh Hung*, 629 F.2d 908, 913 (4th Cir. 1980).

2011] *CAN WE FIND AND STOP THE “JIHAD JANES”?* 125

threats.

The laws of both countries provide a formidable array of tools to seek out intelligence, but before they can be deployed, a potential terrorist has to be brought to the attention of law enforcement authorities. So we are still left with the question of how to find the Jihad Janes in the first place. There is no easy, quick-fix solution to this problem. Many different surveillance techniques are being used at great cost,<sup>227</sup> both in terms of erosion of civil liberties and expenditure of government and taxpayers' money. Nevertheless, the challenge is still to spot potential terrorists *before* their actions bring them to the attention of law enforcement officials, without sacrificing more civil liberties along the way.

---

<sup>227</sup> For a thorough exposition of the cost of counterterrorism methods, see DONOHUE, *supra* note 87.

