2011

Streaming the International Silver Platter Doctrine: Coordinating Transnational Law Enforcement in the Age of Global Terrorism and Technology

Caitlin T. Street

Streaming the International Silver Platter Doctrine: Coordinating Transnational Law Enforcement in the Age of Global Terrorism and Technology

Advances in technology, communications, and transportation have done more to blur international boundaries in the past decade than ever before. As a result, effectively combating transnational crime and terrorism now requires significantly greater cooperation among law enforcement, domestic security, and intelligence agencies on a global scale.[1]

> —Donald Van Duyn, FBI Chief Intelligence Officer
> Statement Before the Senate Committee on Homeland Security and Governmental Affairs, January 8, 2009

The dramatic expansion of technology and globalization over the last thirty years has not only facilitated transnational terrorist operations, but also has transformed the countermeasures utilized by law enforcement and amplified the need for counterterrorism coordination between foreign and domestic authorities. Crucially, these changes have altered the fourth amendment calculus, set out by the international silver platter doctrine, for admitting evidence seized in U.S.-foreign cooperative searches abroad. Under the international silver platter doctrine, courts admit the evidence gathered by foreign authorities abroad unless the unreasonable search is deemed a "joint venture" between U.S. and foreign authorities. Notably, the legal framework governing joint ventures is based on standards and guideposts used when coordination be-

1. *Lessons from the Mumbai Terrorist Attacks—Parts I and II: Hearing Before the S. Comm. on Homeland Sec. and Govt. Aff.*, 111th Cong. 67 (2009) (statement of Donald Van Duyn, Chief Intelligence Officer, Federal Bureau of Investigation), *available at* http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_senate_hearings&docid=f:49484.pdf.

tween different law enforcement entities was almost always physical rather than technological. This Note argues that in the twenty-first century, technology and the pervasive transnational terrorist threat have broadened the scope of the international silver platter doctrine, reduced the impact of its joint venture exception, and consequently rendered the Fourth Amendment, in practice, virtually inapplicable to most transnational terrorism investigations. Applying this antiquated legal doctrine to this novel context narrows the range of activities encompassed in the joint venture exception and in turn allows more evidence gathered in unreasonable searches to be presented in U.S. federal courts. While this Note argues that the rise of international terrorism and heightened transnational law enforcement cooperation demands to some extent a broad international silver platter doctrine and a narrow joint venture exception, it also stresses that at some point Congress must legislate to preserve a baseline of fourth amendment values governing cooperative searches of Americans abroad.

INTRODUCTION

November 26, 2008. It's 8:00 p.m. in Mumbai, India. Ten Pakistani men board inflatable dinghies and travel under the cover of darkness into the port of Colaba. Armed with grenades and assault rifles, they slip into Mumbai undetected, determined to unleash a wave of carnage on the Indian people. However, the Mumbai attackers wield something far more powerful than military weaponry—technology. Among the ammunition in their packs sit Blackberrys and global positioning devices that help them navigate the streets of Mumbai. Through news and possibly social networking sites like Twitter, the terrorists monitor international reaction and keep abreast of the local police countermeasures. The gunmen use these resources to dodge the soldiers sent to stop them, and they paralyze the streets

of Mumbai in a three-day shooting and bombing spree that leaves more than 174 people dead and 300 injured.[2]

Taking full advantage of technology to carry out their attacks,[3] the Mumbai terrorists embody the modern transformation in terrorism tactics and operations spawned by the internet age and globalization. Fortunately, this revolution is accompanied by a counterrevolution in the methods international authorities use to combat these dangers. Law enforcement met twenty-first century terror with sophisticated technologies to identify threats and, most importantly, a significant increase in international coordination of terrorism investigations. Three days after the terrorists' dinghies landed in Mumbai, U.S. authorities were already on the ground organizing the investigation with the Indian government and providing technological support to track down the perpetrators.[4]

---

2. Claudine Beaumont, *Mumbai Attacks: Twitter and Flickr Used To Break News*, TELEGRAPH (U.K.), Nov. 27, 2008, http://www.telegraph.co.uk/news/worldnews/asia/india/3530640/Mumbai-attacks-Twitter-and-Flickr-used-to-break-news-Bombay-India.html; Bruce Schneier, *No Need To Ban Google Earth*, HINDU (India), Jan. 29, 2009, http://www.hindu. com/thehindu/holnus/008200901291050.htm; *Terrorists Turn Technology into Weapon of War in Mumbai*, SUNDAY MAIL (Queensl.), Nov. 29, 2008, http://www.couriermail.com.au/news/world/terrorists-and-technology/story-e6freop6-1111118178210; Emily Wax, *Gunmen Used Technology as a Tactical Tool*, WASH. POST, Dec. 3, 2008, http://www.washingtonpost.com/wp-dyn/content/article/2008/12/02/AR200812020 3519.html.

3. The terrorists studied high-resolution satellite images of the targets including those used for Google Earth maps and evaded tracking with cell phones with multiple SIM cards and satellite phones with voice-over-Internet-protocol phone numbers. Wax, *supra* note 2; *see also* Rahul Bedi, *Mumbai Attacks: Indian Suit Against Google Earth over Image Use by Terrorists*, TELEGRAPH (U.K.), Dec. 9, 2008, http://www.telegraph.co.uk/news/worldnews/asia/india/3691723/Mumbai-attacks-Indian-suit-against-Google-Earth-over-image-use-by-terrorists.html; Rhys Blakely, *Google Earth Accused of Aiding Terrorists*, TIMES (London), Dec. 9, 2008, http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article5311241.ece; Jeremy Kahn & Robert F. Worth, *Mumbai Attackers Called Part of Larger Band of Recruits*, N.Y. TIMES, Dec. 9, 2008, at A14, *available at* http://www.nytimes.com/2008/12/10/world/asia/10mumbai.html; Schneier, *supra* note 2; Margashirsha Krushna Shashthi, *Mumbai Terror Attack E-mails Sent from Pakistan*, HINDU JANAJAGRUTI SAMITI (India), Dec. 17, 2008, http://www.hindujagruti.org/news/5981.html; *Terrorists Turn Technology into Weapon of War in Mumbai*, *supra* note 2; Ginger Thompson & David Johnston, *U.S. Man Accused of Helping Plot Mumbai Attack*, N.Y. TIMES, Dec. 7, 2009, at A1, *available at* http://www.nytimes.com/2009/12/08/world/asia/08terror.html; *U.S. Citizen Charged in Mumbai Attacks*, CNN, Dec. 8, 2009, http://www.cnn.com/2009/ CRIME/12/07/american.mumbai.arrest/index.html.

4. With "unprecedented access to evidence and intelligence related to the attacks," the FBI established 24/7 command posts to process information and conduct interviews and used technological resources, like forensics and surveillance, to assist the Indian authorities

These unprecedented cooperative counterterrorism investigations raise important fourth amendment concerns when they target U.S. citizens abroad. If these searches of U.S. persons fall short of the Fourth Amendment's reasonableness requirement, the little-studied international silver platter doctrine determines whether the evidence gathered can be used in American criminal trials. Under this doctrine, courts admit the evidence unless the unreasonable search is deemed a joint venture between United States and foreign authorities.[5] However, because technology and globalization constrict the legal definition of "joint venture," many collaborative efforts escape constitutional requirements. Nevertheless, this Note argues that the character of the terrorist threat—namely, its global nature and catastrophic potential—requires a narrow joint venture exception and mandates a flexible interpretation of the international silver platter doctrine in order to encourage international cooperation in the War on Terror.

Part I explains how technology has changed both the nature of the terrorist threat and the methods domestic and foreign authorities use to combat this threat. Part II outlines American case law governing the extraterritorial application of the Fourth Amendment and explains how courts applied the silver platter doctrine's joint venture exception prior to the massive revolution in communications and information technology. Part III examines how increased technology and connectivity transformed the test for joint venture. Finally, using this insight, this Note recommends how best to apply the joint venture test to modern transnational terror investigations in light of technological changes, and it defends that interpretation from both substantive and institutional perspectives.

I. THE TECHNOLOGICAL EVOLUTION OF TERRORISM AND LAW ENFORCEMENT IN THE TWENTY-FIRST CENTURY

The dramatic expansion of technology and globalization over the last thirty years has transformed both the operations of terrorist organizations and the countermeasures utilized by law enforcement. Part A explores how increasing interconnectivity and technical innovations have altered the structure and operations of terrorist organizations, facilitated terrorist activities and provided terrorists with new

---

to identify suspects and to uncover possible American connections. *Lessons from the Mumbai Terrorist Attacks—Parts I and II*, *supra* note 1, at 68.

5. United States v. Behety, 32 F.3d 503, 510–11 (11th Cir. 1994).

and unique weaponry. Part B examines how technological growth and globalization have forced law enforcement to undergo an evolution in the investigative techniques that it employs to prevent attacks.

A. Technology Has Changed the Nature of the Terrorism Threat

Since the end of the Cold War, globalization and the rise of information technology have directly paralleled and facilitated the expansion of international terrorism. The "free flow of goods and finances helps terrorists obtain equipment and funds," while "[t]he modern relatively borderless situation means that terrorism can disseminate a psychological state of fear" to people around the world regardless of their citizenship or physical location.[6] Further, technology has fundamentally altered the structure and operations of terrorist organizations, allowing them to operate effectively underground.[7] After 9/11, technology provided Al-Qaeda with a medium to continue their operations and maintain organizational control, "us[ing] the internet to replace their dismantled training camps, reconnect their weakened organization, and reconstitute their leadership," even while being pursued by the most powerful nations in the world.[8]

First, technology and globalization serve as catalysts for secret remote planning and perpetration of terrorist operations.[9] Enhanced communications and internet capabilities facilitate terrorists' efforts to disseminate publicity or propaganda, recruit and mobilize supporters, fundraise, communicate and coordinate with operatives,

---

6. Chin-Huang Lin et al., *Opportunities and Challenges Created by Terrorism*, 74 TECH. FORECASTING & SOC. CHANGE 148, 151 (2007).

7. Technology facilitated evolution from a traditional hierarchal structure to "arrays of transnationally internetted groups." John Arquilla, David Ronfeldt & Michele Zanini, *Networks, Netwar and Information-Age Terrorism*, *in* COUNTERING THE NEW TERRORISM 39, 41 (I.O. Lesser et al. eds., 1999); Maura Conway, *Reality Bytes: Cyberterrorism and Terrorist "Use" of the Internet*, FIRST MONDAY (Nov. 4, 2002), http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1001/922.

8. Jarret M. Brachman, *High-Tech Terror: Al-Qaeda's Use of New Technology*, 30 FLETCHER F. WORLD AFF. 149, 153–54 (2006).

9. As Paul Pillar, a twenty-eight-year CIA veteran, notes: "[i]nformation technology's biggest impact on terrorists has involved the everyday tasks of organizing and communicating, rather than their methods of attack." Lin et al., *supra* note 6, at 153. Scholars have identified an increase in terrorists' use of the internet. JAMES JAY CARAFANO & RICHARD WEITZ, HERITAGE FOUND., COMBATING ENEMIES ONLINE: STATE-SPONSORED AND TERRORIST USE OF THE INTERNET 3 (2008), *available at* http://s3.amazonaws.com/thf_media/2008/pdf/bg2105.pdf; *see also* Lin et al., *supra* note 6, at 151.

gather intelligence on potential targets and share information (e.g., weapons making and training) necessary for planning and carrying out attacks.[10] The internet offers an easily accessible mechanism to spread instantly an extremist message to a worldwide audience at low cost. The internet also facilitates anonymous communications with minimal government surveillance[11] and provides operational flexibility.[12] The web also provides unprecedented information necessary to plan attacks and identify targets, with publicly available resources like Google Earth and social networking sites supplying attackers with intimate details about vulnerable physical locations and high-interest individuals.[13] Communication resources boost coordination among cells, "allowing autonomy at the basic level of this organization—probably only a single individual,"[14] and enable remote control and organization of disparate global cells[15] by "provid[ing] linkage to weapons information, training courses, and inspiration from charismatic leaders globally."[16] By facilitating underground coordi-

10. CARAFANO & WEITZ, *supra* note 9, at 3. RAND scholars Rohfeldt and Arquilla define "netwar" as a form of conflict where the opposition uses "network forms of organization and related doctrines, strategies, and technologies." Evan F. Kohlmann, *The Real Online Terrorist Threat*, 85 FOREIGN AFF. 115, 116 (2006). The key architect of Al-Qaeda's internet movement, Abu Musab al-Suri (responsible for disseminating web propaganda and increasing technology use across cells), has stressed the necessity of the internet in establishing and sustaining the jihad. Brachman, *supra* note 8, at 159.

11. CARAFANO & WEITZ, *supra* note 9, at 4.

12. Many forms of media can be transmitted (e.g., video, text, voice, etc.) through numerous alternate venues (e.g., ISPs, chat rooms, message boards, multiple websites, etc.). *Id.* Terrorist organizations use multiple websites to spread propaganda, gather funds and facilitate communication between underground sects. Ken Berry, *New Weapons Technology*, INT'L COMMISSION ON NUCLEAR NON-PROLIFERATION AND DISARMAMENT, at 6, http://www.icnnd.org/research/New_Weapons_Technology.doc; Conway, *supra* note 7, at 4 tbl.1. The ability to disseminate messages remotely to the international media with little risk of apprehension is unprecedented: "Modern communications technology makes it easy for terrorists to transmit their messages . . . and . . . makes it difficult for the governments to insulate their citizens from the terrorist threats." Lin et al., *supra* note 6, at 153.

13. *See, e.g.*, Jodi Lai, *Terrorists Could Use Facebook Places To Stalk Victims, Security Officials Warn*, NAT'L POST (Canada), Oct. 4, 2010, http://news.nationalpost.com/2010/10/04/terrorists-could-use-facebook-places-to-stalk-victims-security-officials-warn; *see also* Lin et al., *supra* note 6, at 151 (noting that the internet provides "a vast repository of potentially relevant technical information to any individual anywhere on Earth").

14. Lin et al., *supra* note 6, at 151.

15. Al-Qaeda cells have used Google or Yahoo forums, websites and chat rooms to support recruits in organizing new cells. Brachman, *supra* note 8, at 154.

16. Lin et al., *supra* note 6, at 151; *see also* CLAY WILSON, CONG. RESEARCH SERV., RL 32114, BOTNETS, CYBERCRIME, AND CYBERTERRORISM: VULNERABILITIES AND POLICY

nation, the spread of radical ideology and the launch of attacks remotely, technology allows borderless terrorist networks to pose a genuine threat to nations equipped with overpowering military resources.[17]

Second, terrorists can employ technology itself as a weapon or a target in their attacks.[18] Advances in nuclear, biological, chemical and electromagnetic pulse (EMP)[19] weaponry provide unparalleled opportunities for terrorist groups to pose widespread and imminent danger to their targets.[20] Cyberwarfare provides terrorists with a new avenue for operations, because the United States's reliance on internet and computer systems heightens the United States's vulnerability to attacks.[21] For instance, foreign hackers could infiltrate military computer systems to access weapons systems or manipulate tac-

---

ISSUES FOR CONGRESS 19 (2008), *available at* http://www.fas.org/sgp/crs/terror/RL32114.pdf; Brachman, *supra* note 8, at 154; *infra* notes 136–37 and accompanying text. The 9/11 hijackers and planners used the internet and new internet-based phone services to coordinate the attacks. Lin et al., *supra* note 6, at 153–54.

17. The internet provides terrorists with unique opportunities to combine their use of technology for propaganda with their use of technology to launch attacks. Brachman, *supra* note 8, at 154. For instance, a Sunni insurgent group in Iraq developed a competition for redesigning their website where the winner would launch rockets directed at a U.S. military base in Iraq remotely through the internet. *Id.* at 155; Kohlmann, *supra* note 10, at 122. Although the website was shut down before the competition closed, this contest illustrates how technology has fundamentally changed the nature of the terrorist threat—even a website itself can be a technological tool to launch an attack. Brachman, *supra* note 8, at 155; Kohlmann, *supra* note 10, at 122.

18. Conway, *supra* note 7, at 6.

19. EMPs can destroy all electronics systems over a very large area, virtually paralyzing the target city. Berry, *supra* note 12, at 9–11.

20. Experts predict that in the next ten years terrorists will "adapt existing technology and use new technology," including "nuclear, biological, and chemical (NBC) weapons" and "cyber warfare, ranging from viruses to fluid swarm networks and coordinated massive disruption attacks." Lin et al., *supra* note 6, at 151. This evolution in weapons technology extends broadly, including: biotechnology; nanotechnology; invisibility cloaks; unmanned ground combat and aerial combat vehicles; augmented reality; genetics; "giving soldiers internal/biologic infrared, night vision, radar, and sonar capability"; global positioning systems (GPS); force fields; microwave guns; neuroscience; positron bombs; robotic exoskeletons; space-based weapons (ANGELS, Rods from God); telepathy; and "thought control of internet surfing and electronic devices." Berry, *supra* note 12, at 2.

21. Berry, *supra* note 12, at 5 (noting that "cyberwarfare is a significant force equalizer"). From least to most serious, types of cyberterrorism include propaganda and disinformation, web vandalism or Denial of Service (DoS), compromising hardware and cyber espionage. The more threatening Distributed Denial of Service (DDoS) involves using a "botnet" (a network of hundreds of computers) in coordinated attacks against key computer systems of the target. WILSON, *supra* note 16, at 5.

tical decision making[22] by substituting or blocking high-value information or orders, causing catastrophic damage to troops on the ground.[23] Cyber attacks could also shut down computer systems controlling critical infrastructure, cutting off access to power, water, fuel, communications, financial or transportation resources.[24] Thus, technology not only enables terrorists to plan attacks and spread radical ideology remotely but also provides them with weapons that can wreak catastrophic results for relatively low cost.

B. Technology Has Changed the Methods Authorities Use To Combat Terrorism

The technological evolution in the threat to national security demands similar modernization in the countermeasures employed by international and domestic authorities. Enormous strides in technological innovation have equipped more advanced countries with the tools to counteract and undermine terrorist activities. Remarkably, however, many countries that face the strongest threat from terrorism, especially those serving as havens for terrorist planning or those constantly under siege by radical violence, lack the technological weaponry necessary to prevent and deter these extremists. For example, in some Middle Eastern and African countries, the technical

22. Berry, *supra* note 12, at 1.

23. *Id.* at 4–5. Bombing missions by the U.S. Air Force are organized through sophisticated computer-controlled weapons and sensor systems, like "Network Centric Warfare" (NCW), that send satellite photos of targets via email to the air crew. Operational leaders track ground forces on computers and base tactical decisions on these locations. *Id.* at 5–6. Many Department of Defense officials support establishing a "global information grid" (GIG) connecting all advance weapons platforms, the NCW and command and control centers. The GIG would streamline war making and centralize tactical decisions, ideally increasing efficiency and coordinating information, but would increase vulnerability to cyber attack. *Id.* at 6.

24. *Id.* at 5. Cyber attacks over the last two decades have illustrated the grave reality of this threat. In 2005, there were 79,000 attempted hackings into Pentagon computer systems, 1,300 of which were successful. *Id.* at 3. From 2003 to 2006, U.S. and U.K. defense- and security-related computer systems were attacked in an incident known as "Titan Rain." *Id.* at 8. Estonia and Georgia also suffered DDoS attacks in 2007 and 2008 respectively. *Id.* at 4; WILSON, *supra* note 16, at 7–8; Charles Clover, *Kremlin-Backed Group Behind Estonia Cyber Blitz*, FIN. TIMES (U.K.), Mar. 11, 2009, *available at* http://www.ft.com/cms/s/0/57536d5a-0ddc-11de-8ea3-0000779fd2ac.html?nclick_check=1 (by subscription); Ian Traynor, *Russia Accused of Unleashing Cyberwar To Disable Estonia*, GUARDIAN (U.K.), May 17, 2007, http://www.guardian.co.uk/world/2007/may/17/topstories3.russia.

expertise of law enforcement lags behind that of the terrorists. The global reach of terrorism mandates that countries work together to combat it, and doing so often requires sharing the fruits of our technological advances. Section 1 outlines the latest innovations that help law enforcement combat terrorist plots. Section 2 highlights the collaborative efforts to date and illustrates the necessity for international cooperation in developing the technical resources to defeat terror.

1. Technology To Combat Terrorism

Employing sophisticated surveillance and weapons technology is critical in countering the international terrorism threat.[25] First, advanced surveillance systems[26] can intercept and scan global internet and phone communications for suspect transmissions.[27] Law enforcement can also target the contents of specific computers, employing remote searches to infiltrate personal technology systems like computers and email accounts around the world.[28] Second, on the street level, millions of closed-circuit televisions provide essential in-

25. James Jay Carafano, *The Future of Anti-Terrorism Technologies*, Heritage Lectures No. 885, HERITAGE FOUND. (delivered Jan. 17, 2005, published June 6, 2005), http://s3.amazonaws.com/thf_media/2005/pdf/hl885.pdf.

26. Examples include Carnivore (implemented during the Clinton administration to monitor email and electronic communications but reportedly cancelled in 2001) or NarusInsight (a commercial supercomputer system used to perform real-time mass surveillance and monitoring of Internet communications). *FBI Ditches Carnivore Surveillance System*, FOX NEWS, Jan. 18, 2005, http://www.foxnews.com/story/0,2933,144809,00.html; Press Release, Narus, Inc., NarusInsight Intercept Suite Enhanced to Solve Critical Requirements for Targeting, Capturing and Reconstruction of Complex Webmail Traffic (Dec. 10, 2007), *available at* http://www.narus.com/ index.php/news/press-releases/article/127.

27. Kohlmann, *supra* note 10, at 124. Though details are classified, an advanced surveillance system that collects and analyzes signals intelligence (SIGINT) is operated on behalf of the five signatory states to the UK-USA Security Agreement (Australia, Canada, New Zealand, the United Kingdom and the United States), and is reportedly capable of intercepting and analyzing the content of phone conversations, faxes, emails and other data traffic globally by intercepting satellite transmissions. Gerhard Schmid, *Report on the Existence of a Global System for the Interception of Private and Commercial Communications (Interception System)*, at 23 (July 11, 2001), *available at* http://www.europarl.europa.eu/oeil/FindByProcnum.do?lang=2&procnum=INI/2001/2098 (click on link marked "A5-0264/2001" followed by the PDF icon in the pop-up window).

28. Jeremy A. Moseley, Note, *The Fourth Amendment and Remote Searches: Balancing the Protection of "The People" with the Remote Investigation of Internet Crimes*, 19 NOTRE DAME J.L. ETHICS & PUB. POL'Y 355, 356, 363 (2005).

formation for investigating and preventing potential terrorist threats.[29] Further, space-based surveillance systems, namely reconnaissance satellites, provide current images of suspicious locations or potential targets around the world, enabling intelligence and law enforcement officials instantly to gather and transmit information on terrorist threats worldwide.[30] In addition, the United States employs unmanned aerial vehicles (UAVs) or remotely piloted vehicles (RPVs) equipped with sensors and cameras.[31] Intelligence authori-

29. The United Kingdom reportedly has at least four million cameras. *FactCheck: How Many CCTV Cameras?*, CHANNEL 4 NEWS (U.K.), June 18, 2008, http://www.channel4.com/news/articles/society/factcheck+how+many+cctv+cameras/2291167.html; Peter Fry, *How Many Cameras Are There?*, CCTV USER GROUP (June 18, 2008), http://www.cctvusergroup.com/art.php?art=94; Paul Lewis, *Every Step You Take: U.K. Underground Centre That Is Spy Capital of the World*, GUARDIAN (U.K.), Mar. 2, 2009, http://www.guardian.co.uk/uk/2009/mar/02/westminster-cctv-system-privacy; Michael McCahill & Clive Norris, *CCTV in London* (Urbaneye, Working Paper No. 6, June 2002), http://www.urbaneye.net/results/ue_wp6.pdf. A 2006 survey estimates that there are 4,468 cameras in Manhattan alone, up from a 1998 report of 3,000 in New York City. Kevin Anderson, *You're Being Watched, New York!*, BBC NEWS, Mar. 11, 2002, http://news.bbc.co.uk/2/hi/americas/1865828.stm; *Who's Watching?: Video Camera Surveillance in New York City and the Need for Public Oversight*, Special Report, N.Y. C.L. UNION (Fall 2006), http://www.nyclu.org/pdfs/surveillance_cams_report_121306.pdf; *see also Surveillance Camera Project Overview*, NYC SURVEILLANCE CAMERA PROJECT, http://www.mediacater.com/cameras/overview.html. Chicago reportedly has 2,200. Fran Spielman, *Is Chicago Safe from a Terrorist Attack?*, CHICAGO SUN-TIMES, Jan. 8, 2007, http://web.archive.org/web/20070325081308/http:/www.suntimes.com/news/metro/201612,CST-NWS-contro08.article (accessed by searching for the article in the Internet Archive index).

30. *See generally* RICHARD A. BEST JR. & JENNIFER K. ELSEA, CONG. RESEARCH SERV., RL 34421, SATELLITE SURVEILLANCE: DOMESTIC ISSUES 3–4 (2010) (describing applications of satellite-derived intelligence), *available at* http://www.fas.org/sgp/crs/intel/RL34421.pdf. The Department of Homeland Security is responsible for coordinating satellite use. *Id.* The National Reconnaissance Office builds and operates the satellites. NAT'L RECONNAISSANCE ORG., http://www.nro.gov/ (last visited Mar. 18. 2011). For types of satellites, see Emily Clark, *Military Reconnaissance Satellites (IMINT)*, CENTER FOR DEF. INFO. (Oct. 16, 2001), http://www.cdi.org/terrorism/satellites.cfm.

31. Carafano, *supra* note 25, at 4. UAVs equipped with optical sensors can provide clear photograph-like images during any weather condition at any time of day. Electromagnetic spectrum sensors (EMSs) detect sources of energy. Combined with visual spectrum, infrared or near infrared cameras and radar systems, EMSs can generate three-dimensional images of the landscape below that can be enlarged, reduced or rotated without losing image quality. Biological sensors can detect airborne presence of microorganisms, while chemical sensors use laser spectroscopy to analyze concentration of elements in the air. DAVID OMARA, AP LABS, DEPLOYING RUGGEDIZED SYSTEMS IN UNMANNED MILITARY VEHICLES FOR ADVANCED AIR-SEA-LAND APPLICATIONS 3 (2009), *available at* http://www.aplabs.com/pdf/uav-whitepaper-part1.pdf; *see also* JAMES B. CAMPBELL,

ties use the UAVs regularly to receive photographs or data detecting the presence of biological agents, chemicals, explosives or nuclear radiation, providing an essential real-time tool for terrorism investigations[32] and serving as an effective early warning system.[33] Finally, high resolution thermal vision systems, night vision systems, facial recognition software, global positioning systems (GPS) and cell phone tracking technology assist law enforcement in discovering, monitoring and raiding suspected terrorist control centers.[34]

Though reportedly still under development, new high-end counterterrorism technologies, like biometrics, nanotechnology, directed energy systems and cyber defenses may soon (or may already) play an essential role in transnational terrorism investigations. Biometrics technology provides identity verification through recorded physical or behavioral characteristics, such as iris, hand, fingerprint, face or voice recognition, potentially offering essential clues in terrorist investigations.[35] For example, if an optical sensor at a nuclear facility captures an individual's image, law enforcement may identify him as a terrorist suspect by using a facial recognition scan to compare his features against a database of known terrorists.[36] Similarly, if a surveillance system flags a phone call wherein an unnamed individual mentions an attack on an American city, voice recognition

---

INTRODUCTION TO REMOTE SENSING (4th ed. 2008) (describing various forms of remote sensing imagery and their applications).

32. The National Geospatial-Intelligence Agency (NGA) integrates intelligence from satellites with overhead imagery available from NASA satellites, commercial satellites, manned aircraft or unmanned aerial vehicles and airborne platforms. NGA uses the compiled data to develop intelligence information combining imagery and geographic data to develop mapping and elevation models, scene visualization and situation analysis (known as GEOINT). BEST & ELSEA, *supra* note 30, at 4. Satellites can also provide MASINT, intelligence information gathered from analysis of radar, infrared and lasers that can be used to provide evidence of the existence or location of weapons of mass destruction. *Id.* at 4–5.

33. Jennifer L. Brower, *The Terrorist Threat and Its Implications for Sensor Technologies*, *in* ADVANCES IN SENSING WITH SECURITY APPLICATIONS 23, 23–54 (Jim Byrnes & Gerald Ostheimer eds., 2006), *available at* http://www.springerlink.com/content/f6l0775j68357745/fulltext.pdf; *see also* Lin et al., *supra* note 6, at 159–60.

34. Non-lethal weapons, like calmatives or malodorants, allow law enforcement to deflect and combat terrorist attacks with minimal damage to surrounding civilians by controlling crowds. Carafano, *supra* note 25, at 3–4. Advanced explosion-proof and autopilot technologies may also defend against attacks on airplanes, trains and other targets. Lin et al., *supra* note 6, at 159–60.

35. Carafano, *supra* note 25, at 3–4.

36. *See id.* at 4 (describing facial recognition technology).

technology may pinpoint the speaker.[37] Further, advances in nanotechnologies at the atomic and molecular level could lead to the development of virtually undetectable surveillance equipment and highly accurate sensors and markers with countless counterterrorism applications.[38] Also, directed-energy weapons, which emit focused beams of energy consisting of electromagnetic radiation such as lasers or microwave radiation at a target, would empower law enforcement to stop threatening vehicles by short-circuiting their electronics.[39] Through defensive cybertechnologies,[40] like the United States's Clandestine Technical Collection program, law enforcement can penetrate computer systems used by transnational terrorist networks, passively intercept communications to identify cells and determine their activities or disrupt terrorist operations by denying services, hacking computer programs and altering messages.[41]

Information technology also plays an essential role in combating terrorism.[42] In order to connect the dots, policy makers must sift

37. *See id.* (describing voice recognition technology).

38. *Id.* at 5–6; *Israeli Nanotech Sensor "Smell" Hidden Bombs Better than Sniffer Dogs*, CHINA DAILY, Nov. 3, 2010, http://www.chinadaily.com.cn/xinhua/2010-11-03/content_1135305.html; John R. Quain, *Nanotechnology May Aid Homeland Security*, ABC NEWS, Dec. 29, 2010, http://abcnews.go.com/Technology/ZDM/story?id=97437&page=1.

39. Nicke Lewer & Neil Davison, *Non-Lethal Technologies—An Overview*, FAS DISARMAMENT FORUM, 42 (2005), http://www.fas.org/programs/bio/chemweapons/documents/Lewer%20and%20Davison.pdf. These weapons, which consist of lasers and microwave radiation emitters, can protect critical infrastructure like airplanes by aiming high power laser beams from miles away to destroy a threat, such as a satellite, missile, aircraft or tank. *Id.* at 6–7.

40. In 2007, McAfee Computer Security Company reported that at least 120 countries were developing cyberwarfare capabilities, focusing on financial markets, corporations, government computer systems and public utilities as targets. Berry, *supra* note 12, at 4. Russia, China, India and Cuba have admitted to developing these cyberwarfare capabilities; while North Korea, Libya, Iran and Syria are suspected of doing so, and the United States, the United Kingdom, France, Germany and Japan already have advanced cyberwarfare technologies. *Id.* The U.S. and foreign governments have worked to develop defenses against this growing cyberwarfare threat, but take an ad hoc approach, focusing on military computer systems rather than industrial and financial institutions. *Id.* at 7; *see* CARAFANO & WEITZ, *supra* note 9, at 4–7 (detailing the response of the United States to cyberterrorism); *see also* John Rollins & Clay Wilson, *Terrorist Capabilities for Cyberattack: Overview and Policy Issues*, *in* 9 FOCUS ON TERRORISM 43 (Edward V. Linden ed., 2007).

41. *See infra* note 161 and accompanying text. For methods to enhance cyber security, see CARAFANO & WEITZ, *supra* note 9, at 4.

42. Robert Popp et al., *Countering Terrorism Through Information Technology*, 47 COMM. OF THE ACM 36, 38 (2004).

through enormous amounts of information, process and analyze it and take action.[43] System integration technologies coordinate networking sensors, policy makers, law enforcement officials and emergency responders to streamline decision making and increase efficiency, security and coordination with foreign intelligence services and all branches of government.[44] In addition, data mining and link analysis technologies identify patterns and anomalies in datasets in order to predict future threats or identify suspect relationships.[45] While the examples above include just a fraction of the unclassified national security technology in development, these advances illustrate the range of sophisticated technological tools available to U.S. law enforcement in counterterrorism investigations.

2. Helping Countries That Fall Behind the Technology Curve

While scientifically advanced countries can use these tools to combat terrorism, technologically unsophisticated countries are ill-equipped to deal with attacks. A 2006 RAND study on the levels of technological development across countries shows a lag in Middle Eastern, African and South Asian countries—areas that are also plagued by terrorist activity.[46] During the Mumbai attacks, for example, the Indian authorities were severely disadvantaged by their failure to keep up with the terrorists' use of technology. Equipped with weapons from the 1940s, the local police were not able effectively to combat the technical expertise and savvy the terrorists employed to plan and execute the strikes.[47] Indian security forces such as the Black Cats did not have access to night-vision goggles or thermal-imaging capability, and the National Security Guard did not have its own aircraft.[48] Even when the authorities had the technological resources, they did not employ them effectively. For example, the local authorities did not monitor the few closed-circuit televisions

43. *Id.*

44. Carafano, *supra* note 25, at 3. Popp et al., *supra* note 42, at 40 (arguing that using information technology to gather information allows analysts to devote more time to analyzing and thinking about how the dots connect).

45. Link analysis, also known as description, works to find commonalities in data to identify relationships between individuals and organizations, allowing analysts to isolate suspect relationships to prevent terror attacks. Carafano, *supra* note 25, at 5.

46. RAND CORP., GLOBAL TECHNOLOGY REVOLUTION 2020 (2006), *available at* http://www.rand.org/content/dam/rand/pubs/research_briefs/2006/RAND_RB9179.pdf.

47. *See* Wax, *supra* note 3.

48. *Id.*

in operation during the attacks, missing the opportunity to either alert authorities before the attacks or identify suspects afterwards.[49] Similarly, without international assistance, many countries lack the resources to identify, track and apprehend technologically sophisticated terrorists. The United States has instituted counterterrorism assistance programs, bolstered intelligence partnerships and enhanced technological sharing with foreign partners in an effort to prevent attacks.

The technological barriers faced by foreign law enforcement magnify the danger of transnational terrorism and highlight the imperative need for cooperative counterterrorism efforts. The U.S. government has initiated a number of international assistance programs through the Department of Defense,[50] the Department of State[51] and the Department of Homeland Security,[52] that provide

---

49. *Id.*

50. The Department of Defense's security assistance programs include: foreign military sales, international military education and training (IMET), transfers of excess defense articles, foreign military financing (including NATO's Partnership for Peace, the African Crisis Response Initiative and the Enhanced International Peacekeeping Initiative) and the Technical Cooperation Program (where scientists from the United States, the United Kingdom, Australia, New Zealand and Canada work on defense projects, conduct joint experiments and collaborate on research and development through the sharing of data, equipment and facilities). JAMES JAY CARAFANO & RICHARD WEITZ, HERITAGE FOUND., ENHANCING INTERNATIONAL COLLABORATION FOR HOMELAND SECURITY AND COUNTERTERRORISM 2–3 (2007), *available at* http://s3.amazonaws.com/thf_media/2007/pdf/bg2078.pdf.

51. The Department of State offers comprehensive foreign assistance counterterrorism programs designed to build institutions, train law enforcement and develop the rule of law. Programs include: the Antiterrorism Training Assistance (ATA) (which trains foreign law enforcement in hostage negotiations, bomb detection, airport security, investigating terrorism and cyberterrorism, develops international networks among U.S. and foreign counterterrorism experts and law enforcement, and has trained over 48,000 foreign security officials from over 141 countries since 1983); the Terrorist Interdiction Program (TIP) (improves border security in terror-laden countries by equipping local officers with a sophisticated database system and training support to identify and track suspected terrorists and is operational in eighteen countries in 2005, extended to five more by 2006); CT Engagement program (strengthens international counterterrorism cooperation through bilateral conferences); Counterterrorism Finance Capacity Building (provides countries with technical assistance in drafting anti-terrorist financing legislation; and trains bank regulators, investigators and prosecutors to identify and combat financial terror crimes); and country-specific aid. *See Foreign Operations, Export Financing, and Related Programs Appropriations for Fiscal Year 2005: Hearing Before a Subcomm. of the S. Comm. on Appropriations on H.R. 4818/S. 2812*, 108th Cong. 137–40 (2005) (statement of Cofer Black, Coordinator for Counterterrorism, Department of State), *available at* http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_senate_hearings&docid=f:92146.pdf; *Counterterrorism Blog & Potomac Institute Panel: Reforming U.S.*

technological resources essential for foreign development, education, humanitarian assistance, military training and financing and aviation and maritime security assistance.[53] In addition, the U.S. Intelligence Community (IC) maintains many foreign intelligence relationships that provide domestic and foreign law enforcement with information to combat terrorist threats. Through liaison relationships, certain countries have "access to intelligence and can implement direct action that the U.S. requires to pursue its national security interests."[54] International cooperation between intelligence services can be both formal and ad hoc. For example, formal cooperation between the United States and the United Kingdom in 2006 prevented a plot to destroy several planes over the Atlantic. [55] The United States has formalized special intelligence relationships with the United Kingdom, Canada, Australia and New Zealand whereby they share information and conduct a high level annual meeting.[56] A more ad hoc relationship between the United States and Pakistani intelligence services facilitated the capture of Khalid Sheikh Mohammed in 2003.[57]

International coordination in counterterrorism technologies has increased after 9/11, as the United States has recognized the vitality of transnational information and technology sharing in order to prevent attacks. The U.S. Defense Advanced Research Projects Agency (DARPA) took steps to collaborate with and within foreign intelligence and counterterrorism communities through information technology to identify threats more quickly by sharing information,

---

Counterterrorism Assistance Programs, COUNTERTERRORISM BLOG, 4–5 (Feb. 12, 2008), http://counterterrorismblog.org/Reforming%20U.S.%20Counterterrorism%20Assistance%20Programs_CTB%20Event%202.pdf; CARAFANO & WEITZ, *supra* note 50, at 4.

52. CARAFANO & WEITZ, *supra* note 50, at 4–5.

53. *Id.* at 1–2.

54. ERIC ROSENBACH & AKI J. PERITZ, CONFRONTATION OR COLLABORATION? CONGRESS AND THE INTELLIGENCE COMMUNITY 50 (2009), *available at* http://belfercenter.ksg.harvard.edu/files/IC-book-finalasof12JUNE.pdf.

55. *Id.* at 51.

56. *Id.*

57. *Id.* The United States also has intelligence relationships with non-state actors, including tribal groups, political parties and specialized security organizations. For instance, the United States, Pakistan's Inter-Services Intelligence (ISI) and Saudi Arabia worked together to fund and train Afghans to fight the Soviets in the 1980s. Today, the ISI helps the United States locate Islamic extremists, Taliban operatives and Al-Qaeda leaders. The United States and Sudan also have a counterterrorism agreement; American and Sudanese intelligence offices collaborated in the hunt for Bin Laden in the 1990s when he lived in Khartoum. Recently, Sudan has helped track Al-Qaeda operatives. *Id.* at 52.

which leads to better analyses and more informed decision making.[58] Countries have also created Joint Standing Committees on counter-terrorism and technology cooperation,[59] formalized international agreements to cooperate on fighting cybercrime[60] and collaborated with academics and world leaders on national security technology during international workshops.[61] As one scholar puts it, "technological developments and their availability as spread by the globalized market economy have unavoidably expanded the dangers of terrorism in the new century."[62] Clearly, the United States must "rely on other countries together to encircle and suppress domestic terrorist activity."[63] While globalization reduces the ability of governments to control the flow of information, especially that regarding people, property and military weaponry, globalization also provides new opportunities for the United States to work with international partners in combating terrorism: "There are no frontiers in 21st century national security. Distinguishing clear lines of responsibility between foreign and domestic security is a thing of the past."[64]

---

58. *See* Marshall Billingslea, *Military Matters: Combating Terrorism Through Technology*, NATO REV. (Autumn 2004), http://www.nato.int/docu/review/2004/issue3/english/military.html; Popp et al., *supra* note 42, at 36. The United Kingdom's Home Office has taken similar measures through the International Collaboration Plan. HM GOVERNMENT, THE UNITED KINGDOM'S SCIENCE AND TECHNOLOGY STRATEGY FOR COUNTERING INTERNATIONAL TERRORISM 21 (2009).

59. *See, e.g.*, U.S. COMM. ON STRENGTHENING U.S. & RUSS. COOP. NUCLEAR NONPROLIFERATION & RUSS. COMM. ON STRENGTHENING U.S. & RUSS. COOP. NUCLEAR NONPROLIFERATION, STRENGTHENING U.S.-RUSSIAN COOPERATION ON NUCLEAR NONPROLIFERATION (2005), *available at* http://www.nap.edu/catalog.php?record_id=11302 (report issued by joint committee staffed by members of the U.S. National Academies and the Russian Academy of Sciences).

60. *See* WILSON, *supra* note 16, at 32. After the cyber attacks on Estonia, NATO deployed Computer Emergency Response Teams (CERTs) which organized work for foreign ISPs, local law enforcement and network managers to create a coordinated response from information infrastructure, which significantly limited the effects of the attack. *See* CARAFANO & WEITZ, *supra* note 9, at 6.

61. T.G.K Murthy & John Holdren, *Discussion of Indo-U.S. Cooperation*, *in* SCIENCE AND TECHNOLOGY TO COUNTER TERRORISM: PROCEEDINGS OF AN INDO-U.S. WORKSHOP 151, 151–52 (Roddam Narasimha et al. eds., 2007), *available at* http://books.nap.edu/openbook.php?record_id=11848&page=151.

62. Lin et al., *supra* note 6, at 154.

63. *Id.*

64. *Id.*

II. COORDINATING CRIMINAL INVESTIGATIONS ACROSS BORDERS: THE EXTRATERRITORIAL APPLICATION OF THE FOURTH AMENDMENT AND THE INTERNATIONAL SILVER PLATTER DOCTRINE

The rise of international crime, like drug trafficking, antitrust violations and terrorism, has increased the need for transnational law enforcement cooperation.[65] In order to prosecute these crimes, U.S. courts have increasingly evaluated evidence seized by foreign police abroad. In these cases, questions about the extraterritorial application of the Fourth Amendment's protection against "unreasonable searches and seizures" often arise.[66] This Section first outlines American case law governing the extraterritorial application of the Fourth Amendment, focusing on the silver platter doctrine. The Note then explains how courts applied the joint venture exception prior to the massive technological growth of the last thirty years.

A. Extraterritorial Application of the Constitution and the Fourth Amendment

The Fourth Amendment protects individuals against "unreasonable searches and seizures" conducted by the federal government.[67] The Supreme Court interprets the Amendment to require the

65. *See* Jonathan F. Lenzner, *From a Pakistani Stationhouse to the Federal Courthouse: A Confession's Uncertain Journey in the U.S.-Led War on Terror*, 12 CARDOZO J. INT'L & COMP. L. 297, 297–98 (2004) (noting the unprecedented cooperation between the United States and foreign governments in terrorism investigations) (citing Michael Ware, *Taunts From the Border*, TIME, Oct. 28, 2002, http://www.time.com/time/magazine/article/0,9171,1003518,00.html); Irvin B. Nathan, *Preventing Disclosure of Grand Jury Materials to Foreign Governments Pursuant to MLATS*, 8 BUS. CRIMES BULL. 1, 1 (2001); *see also* Christopher D. Man, *Extradition and Article III: A Historical Examination of the Judicial Power of the United States*, 10 TUL. J. COMP. & INT'L L. 37 (2002) (discussing the constitutionality of the Extradition Act with the premise that transnational law enforcement cooperation is a necessity).

66. "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. CONST. amend. IV.

67. *Id.* (incorporated into the Due Process Clause of the Fourteenth Amendment and applicable to the states through *Wolf v. Colorado*, 338 U.S. 25, 27–28 (1949), *overruled on other grounds by* Mapp v. Ohio, 367 U.S. 643, 654 (1961)).

exclusion of illegally obtained evidence from trial,[68] in order to deter illegal activity by the police. Thus, foreign police are not subject to the Fourth Amendment's restraints because domestic laws will not influence their activity.[69] However, the actions of U.S. law enforcement abroad are still governed, to some extent, by the Fourth Amendment.[70]

At the end of the nineteenth century, the Court held that the Constitution and Fourth Amendment only shielded citizens and other individuals within the United States and not those abroad.[71] However, changing course in *Reid v. Covert,* a majority of the Court extended Fifth and Sixth Amendment protections to Americans abroad, and a plurality held that the Bill of Rights applied to U.S. citizens in other countries.[72] The Court later held that the Fourth Amendment protects Americans abroad from unreasonable searches and seizures if there is sufficient American involvement with the foreign search.[73]

---

68. *Weeks v. United States*, 232 U.S. 383, 392 (1914), *overruled by* Mapp v. Ohio, 367 U.S. 643 (1961), established the exclusionary rule for evidence gathered in unreasonable searches and seizures; this rule was not applied to the states until *Mapp*. *Mapp,* 367 U.S. at 655 (1961).

69. United States v. Rosenthal, 793 F.2d 1214, 1230 (11th Cir. 1986) (describing as "doubtful" the "deterrent effect on foreign police practices that will follow from a punitive exclusion of the evidence in question from an American court"); United States v. Maher, 645 F.2d 780, 782–83 (9th Cir. 1981) ("Neither our Fourth Amendment nor the judicially created exclusionary rule applies to the acts of foreign officials.") (citing United States v. Rose, 570 F.2d 1358, 1361 (9th Cir. 1978)); Stonehill v. United States, 405 F.2d 738, 743 (9th Cir. 1968), *cert. denied*, 395 U.S. 960 (1969); Commonwealth v. Wallace, 248 N.E.2d 246, 247–48 (Mass. 1969) (commenting that the Fourth Amendment is not "directed at foreign police, and no purpose would be served by applying the exclusionary rule, since what we do will not alter the search and seizure policies of the foreign nation").

70. *See* Powell v. Zuckert, 366 F.2d 634, 638 (D.C. Cir. 1966).

71. Ross v. McIntyre, 140 U.S. 453, 464 (1891).

72. Reid v. Covert, 354 U.S. 1, 5–6 (1957) ("The United States is entirely a creature of the Constitution. Its power and authority have no other source. It can only act in accordance with all the limitations imposed by the Constitution. When the Government reaches out to punish a citizen who is abroad, the shield which the Bill of Rights and other parts of the Constitution provide to protect his life and liberty should not be stripped away just because he happens to be in another land.").

73. *See* United States v. Conroy, 589 F.2d 1258, 1265 (5th Cir 1979); United States v. Rose, 570 F.2d 1358, 1362 (9th Cir. 1978). Notably, this rule applies to law enforcement and criminal investigatory searches but may not apply to intelligence searches since lower courts have found an intelligence exception to the Fourth Amendment. In *United States v. Bin Laden*, 126 F. Supp. 2d 264, 273 (S.D.N.Y. 2000), the court held that no warrant was required for search by the U.S. government of an American living abroad when the search is primarily for foreign intelligence purposes rather than a criminal investigation. Further, *In*

The Supreme Court addressed the application of the Fourth Amendment to foreign searches of foreign nationals in *United States v. Verdugo-Urquidez*.[74] In that case, Drug Enforcement Agency (DEA) agents and Mexican Federal Judicial Police conducted a warrantless search of a home in Mexico belonging to a Mexican citizen who was suspected of drug smuggling and ordering the murder of a DEA agent.[75] Though the individual was in an American prison waiting to stand trial during the search, the Court ruled that the Fourth Amendment did not apply.[76] The Court held the Fourth Amendment inapplicable to foreign searches involving aliens with no voluntary connection to the United States.[77] The plurality opinion reasoned that "the people" referred only to people connected to the United States, those who are "part of a national community or who have otherwise developed sufficient connection with this country to be considered part of that community."[78]

The three dissenters argued that if U.S. authorities conducted the foreign search, then the Fourth Amendment and the exclusionary rule should apply when the defendant is criminally prosecuted in U.S. courts because "he has effectively been treated as one of 'the governed.'"[79] The concurrences of Justices Kennedy and Stevens did not find the Fourth Amendment inapplicable as a whole, but rather reasoned that the warrant requirement did not apply in this case because U.S. magistrates do not have the power to initiate warrants abroad.[80] Unlike the plurality, Justice Stevens argued that "the people" in the

---

re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1012 (For. Intel. Surv. Rev. 2008) found an exception when surveillance is conducted to gather foreign intelligence and directed against foreign powers or agents of foreign powers reasonably believed to be located outside of the United States, even if American citizens. *See generally* Corey M. Then, *Searches and Seizures of Americans Abroad: Re-Examining the Fourth Amendment's Warrant Clause and the Foreign Intelligence Exception Five Years After* United States v. Bin Laden, 55 DUKE L.J. 1059 (2006).

74. United States v. Verdugo-Urquidez, 494 U.S. 259 (1990).

75. *Id.* at 262.

76. *Id.* at 274–75.

77. *Id.*

78. *Id.* at 265. The Court also noted that at the founding, the framers designed the Constitution to protect the people of the United States. History shows that the founding generation repeatedly authorized action against aliens abroad without applying the Fourth Amendment. *Id.* at 266–68.

79. *Id.* at 297 (Blackmun, J., dissenting).

80. *Id.* at 278 (Kennedy, J., concurring); *id.* at 279 (Stevens, J., concurring).

Fourth Amendment included any alien "lawfully present in the United States."[81] Since the plurality reasoning did not command a majority, the case did not completely remove the role of the Fourth Amendment in searches of aliens outside of the United States. The three dissents and two concurrences actually leave open the possibility that the silver platter doctrine's joint venture analysis may apply to searches of aliens abroad, just not to searches of individuals under the same facts as *Verdugo-Urquidez*.

In the aftermath of the *Verdugo-Urquidez* decision, courts and academics were uncertain who was entitled to Fourth Amendment protections abroad.[82] While protections ran to U.S. citizens and not to foreign nationals who had only a brief, involuntary physical presence in the United States, the extent of the protections afforded to those in between was unsettled, especially since the plurality defined the "sufficient connection" vaguely.[83] In fact, some lower courts

81. *Id.* at 279 (Stevens, J., concurring).

82. *See* Ronald J. Sievert, *Meeting the Twenty-First Century Terrorist Threat Within the Scope of Twentieth Century Constitutional Law*, 37 HOUS. L. REV. 1421, 1432 (2000) (noting that "Verdugo-Urquidez not only excluded aliens from the shelter of the Fourth Amendment in the course of foreign searches by United States authorities (and potentially during domestic searches), it also pointedly raised questions as to the degree of protection provided to American citizens abroad as well."); *see also* Eric Bentley, Jr., *Toward an International Fourth Amendment: Rethinking Searches and Seizures Abroad After* Verdugo-Urquidez, 27 VAND. J. TRANSNAT'L L. 329 (1994); Christina Duffy Burnett, *A Convenient Constitution? Extraterritoriality After* Boumediene, 109 COLUM. L. REV. 973 (2009); James G. Connell, III & René L. Valladares, *Search and Seizure Protections for Undocumented Aliens: The Territoriality and Voluntary Presence Principles in Fourth Amendment Law*, 34 AM. CRIM. L. REV. 1293 (1997); Ian R. Conner, *Peoples Divided: The Application of the United States Constitutional Protections in International Criminal Law Enforcement*, 11 WM. & MARY BILL. RTS. J. 495 (2002); Eric B. Fisher, *The Road Not Taken: The Extraterritorial Application of the Fourth Amendment Reconsidered*, 34 COLUM. J. TRANSNAT'L L. 705 (1996); Douglas I. Koff, *Post-*Verdugo-Urquidez*: The Sufficient Connection Test—Substantially Ambiguous, Substantially Unworkable*, 25 COLUM. HUM. RTS. L. REV. 435 (1994); Arthur J. Kyriazis & Harry M. Caldwell, *Unchecked Discretion, the Buck Stops Here: Is There a Fourth Amendment at the International Borders of the United States?*, 14 WHITTIER L. REV. 613 (1993); Mark Andrew Marionneaux, *International Scope of Fourth Amendment Protections:* United States v. Verdugo Urquidez, 52 LA. L. REV. 455 (1991); Randall K. Miller, *The Limits of U.S. International Law Enforcement After* Verdugo-Urquidez*: Resurrecting* Rochin, 58 U. PITT. L. REV. 867 (1997); Mary Lynn Nicholas, United States v. Verdugo-Urquidez*: Restricting the Borders of the Fourth Amendment*, 14 FORDHAM INT'L L. J. 267 (1991); Michael Scaperlanda, *The Domestic Fourth Amendment Rights of Aliens: To What Extent Do They Survive* United States v. Verdugo Urquidez*?*, 56 MO. L. REV. 213 (1991); Then, *supra* note 73.

83. Mark Mermelstein, *Searching Far and Wide*, L.A. LAW., Nov. 2003, at 33, 36, *available at* http://www.lacba.org/Files/LAL/Vol26No8/1450.pdf. One scholar suggests that

have modified the test applicable to joint searches of U.S. citizens abroad, moving towards a more flexible reasonableness standard. The Second Circuit recently held that the fourth amendment warrant requirement does not apply in foreign countries even to searches directed at U.S. citizens,[84] stressing that "such searches of U.S. citizens need only satisfy the Fourth Amendment's requirement of reasonableness."[85] Relying on the assertions of the seven justices in *Verdugo-Urquidez* that U.S. courts cannot issue warrants for foreign searches, the court found the electronic surveillance and physical search of a U.S. citizen's home in Nairobi, conducted by U.S. authorities in coordination with Kenyan officials pursuant to a Kenyan warrant authorizing the search (but not a U.S. warrant), reasonable under the Fourth Amendment.[86] Thus, the future application of the Fourth Amendment to searches conducted by U.S. and foreign authorities abroad is far from clear. As a result of this ambiguity, both citizens and aliens subjected to these searches abroad are likely to argue for suppression under the Fourth Amendment based on the joint venture exception to the international silver platter doctrine.

B. Foreign Police Searches and the International Silver Platter Doctrine

The exclusionary rule requires suppression of evidence that U.S. agents gather abroad when the search or seizure violates the Fourth Amendment.[87] The exclusionary rule and the Fourth

---

the following factors determine whether an alien's connection with the United States activates fourth amendment protections: "Whether the alien 1) maintains a place of residence within the United States, 2) owns property within the United States, 3) pays U.S. taxes, 4) has resided within the United States, and 5) has been absent for only a limited time from the United States and intends to return." *Id.* Decisions after *Verdugo-Urquidez* have found that the Fourth Amendment does not apply to searches of non-resident aliens in international waters. United States v. Aikins, 946 F.2d 608, 613 (9th Cir. 1990); *see also* United States v. Bravo, 480 F.3d 88, 96 (1st Cir. 2007); United States v. Zakharov, 468 F.3d 1171, 1179–80 (9th Cir. 2006); United States v. Davis, 905 F.2d 245, 250 (9th Cir. 1990).

84. *In re* Terrorist Bombings of U.S. Embassies in E. Afr., 552 F.3d 157, 167–71 (2d Cir. 2008).

85. *Id.* at 167.

86. *Id.*

87. Powell v. Zuckert, 366 F.2d 634, 639–41 (D.C. Cir. 1966); United States v. Jordan, 1 M.J. 145, 147–49 (C.M.A. 1975); *see also* Steven M. Kaplan, *The Applicability of the Exclusionary Rule in Federal Court to Evidence Seized and Confessions Obtained in Foreign Countries*, 16 COLUM. J. TRANSNAT'L L. 495, 495 (1977) ("It seems accepted that

Amendment, however, do not apply to searches conducted entirely by a foreign government.[88] Therefore, if foreign police independently search an American citizen abroad under standards that would not have met fourth amendment requirements if conducted by U.S. authorities, the evidence acquired in that search could be admitted in a U.S. court.[89] The rule providing for the admissibility of evidence seized by foreign governments and subsequently given to U.S. law enforcement is known as the "international silver platter doctrine." There are two exceptions to the silver platter doctrine: first, when U.S. agents abroad and a foreign government conduct the search or seizure as a joint venture;[90] and second, when the conduct of the foreign government is so horrible that it "shocks the conscience" of the American court.[91] When either of these exceptions is present, the Fourth Amendment governs the acts of the foreign officials and the exclusionary rule applies.[92]

Successful investigation of terrorist threats requires transnational law enforcement cooperation, thus amplifying the importance of the joint venture exception. A three-part analysis determines the

---

evidence obtained abroad as a result of operations violating the fourth or fifth amendments and conducted wholly by American agents will be excluded from federal court.").

88. United States v. Janis, 428 U.S. 433, 455–56 n.31 (1976); United States v. Mount, 757 F.2d 1315, 1317 (D.C. Cir. 1985); United States v. Morrow, 537 F.2d 120, 139 (5th Cir. 1976) ("[T]he Fourth Amendment exclusionary rule does not apply to arrests and searches made by foreign authorities on their home territory and in the enforcement of foreign law, even if the persons arrested and from whom the evidence is seized are American citizens."), *cert. denied*, 430 U.S. 933 (1977).

89. United States v. Mitro, 880 F.2d 1480, 1482 (1st Cir. 1989); United States v. LaChapelle, 869 F.2d 488, 489–90 (9th Cir. 1989); United States v. Rosenthal, 793 F.2d 1214, 1230 (11th Cir. 1986); Commonwealth v. Wallace, 248 N.E.2d 246, 247–48 (Mass. 1969).

90. United States v. Behety, 32 F.3d 503, 510–11 (11th Cir. 1994).

91. United States v. Barona, 56 F.3d 1087, 1091 (9th Cir. 1995); *see also Mitro*, 880 F.2d at 1483–84 ("Circumstances that will shock the conscience are limited to conduct that 'not only violates U.S. notions of due process, but also violates fundamental international norms of decency.'" (quoting Stephen A. Saltzburg, *The Reach of the Bill of Rights: Beyond the Terra Firma of the United States*, 20 VA, J. INT'L L. 741, 775 (1980))). While the exception is rarely found, the Court has held that pumping a suspect's stomach to get two morphine pills, which are later introduced as evidence at trial, "shocks the conscience." Rochin v. California, 342 U.S. 165, 172 (1951).

92. *Barona*, 56 F.3d at 1091 (quoting United States v. Maher, 645 F.2d 780, 782 (9th Cir. 1981)). *See* W.J.A., *The New International "Silver Platter" Doctrine: Admissibility in Federal Courts of Evidence Illegally Obtained by Foreign Officers in a Foreign Country*, 2 N.Y.U. J. INT'L L. & POL. 280 (1969).

admissibility of evidence seized from collaborative efforts.[93] First, the court assesses whether the participation of American agents is substantial enough to be a joint venture.[94] If so, the court evaluates whether the search obeyed foreign law.[95] Law of the locality where the search occurs "governs whether the search was reasonable"[96] and "compliance with the foreign law alone determines whether the search violated the Fourth Amendment."[97] Finally, if the search does not comply with foreign law, the court must determine whether U.S. agents acted on a reasonable belief that the foreign search complied with the foreign country's law.[98] In the foreign search context, the good faith exception to the exclusionary rule means that suppression is not required when U.S. officials rely sincerely on a foreign official's assertion that he had authority to conduct the search.[99]

The lower courts, however, have not agreed on what constitutes a joint venture. All the circuits have adopted different rules, which include one or a combination of the following:

1. *"Substantial participation" of U.S. official*: Under this standard, fact-specific analysis determines if U.S. officials' involvement is "substantial" enough to trigger the Fourth Amendment.[100]
2. *Foreign authorities are "acting as agents" of federal government*: Under this rubric, if U.S. officials request, are present at and participate in the search, and if foreign officials "act[ed] as agents for their American counterparts," then the collabora-

93. United States v. Ferguson, 508 F. Supp. 2d 1, 2 (D.D.C. 2007) (citing *Barona*, 56 F.3d at 1092–93); Kristopher A. Nelson, *Transnational Wiretaps and the Fourth Amendment*, 36 HASTINGS CONST. L.Q. 329, 345 (2009).

94. *See* United States v. Angulo-Hurtado, 165 F. Supp. 2d 1363, 1371 (N.D. Ga. 2001) (noting the high threshold).

95. *See* Nelson, *supra* note 93, at 347.

96. *See Barona*, 56 F.3d at 1092–93; United States v. Peterson, 812 F.2d 486, 491 (9th Cir. 1987); *see also* Sievert, *supra* note 82, at 1435 (arguing that *Barona*'s elaboration of the joint venture doctrine is consistent with the flexible approach to probable cause).

97. *Barona*, 56 F.3d at 1093 (citing *Peterson*, 812 F.2d at 491). But the burden of determining the content of foreign law is on the defendant. *See* Nardone v. United States, 308 U.S. 338, 341 (1939); *Angulo-Hurtado*, 165 F. Supp. 2d at 1372.

98. *See* Nelson, *supra* note 93, at 348–49.

99. United States v. Leon, 468 U.S. 897, 923 (1984).

100. *Barona*, 56 F.3d at 1092.

tion is a joint venture and the Fourth Amendment applies.[101]

3. *"Evading the constitution"*: Finally, under this test, if U.S. officials use the foreign government as a tool to circumvent the Constitution, then that is a joint venture and the Fourth Amendment applies.[102]

Though the standard differs among the circuits, the following acts have not been considered substantial enough to constitute a joint venture under any of them: observing the search and seizure and cooperating slightly;[103] requesting but not participating in foreign search;[104] "trigger[ing] the interest" of foreign authorities who later conduct search and give evidence to the United States;[105] relaying tips which lead to foreign police starting an investigation;[106] passing on information requested by foreign governments;[107] joining foreign police in a foreign-initiated search;[108] participating in foreign wiretaps, as long as U.S. agents did not "initiate, control or direct" them;[109] using information from an illegal foreign wiretap to support a U.S. search warrant;[110] triggering and then participating in a foreign search;[111] and assisting the foreign search but not contributing "substantial resources, such as the provision of translation and decod-

101. United States v. Behety, 32 F.3d 503, 510 (11th Cir. 1994).

102. United States v. Maturo, 982 F.2d 57, 61 (2d Cir. 1992); United States v. Delaema, 583 F. Supp. 2d 104, 107 (D.D.C. 2008).

103. Roberto Iraola, *A Primer on Legal Issues Surrounding the Extraterritorial Apprehension of Criminals*, 29 AM. J. CRIM. L. 1, 17 n.83 (2001).

104. State v. Barajas, 238 N.W.2d 913, 915–16 (Neb. 1976).

105. United States v. Wolfish, 525 F.2d 457, 463 (2d Cir. 1975), *cert. denied*, 423 U.S. 1059 (1976).

106. United States v. Rose, 570 F.2d 1358, 1362 (9th Cir. 1978); United States v. Morrow, 537 F.2d 120, 139–40 (5th Cir. 1976); Brulay v. United States, 383 F.2d 345, 348 (9th Cir. 1967), *cert. denied*, 389 U.S. 986 (1967).

107. United States v. Delaplane, 778 F.2d 570, 573–74 (10th Cir. 1985), *cert. denied*, 479 U.S. 827 (1986); United States v. Phillips, 479 F. Supp. 423, 431–32 (M.D. Fla. 1979).

108. United States v. Rosenthal, 793 F.2d 1214, 1230–31 (11th Cir. 1986); United States v. Benedict, 647 F.2d 928, 930 (9th Cir. 1981).

109. United States v. Cotroni, 527 F.2d 708, 712 (2d Cir. 1975), *cert. denied*, 426 U.S. 906 (1976).

110. United States v. Maher, 645 F.2d 780, 783 (9th Cir. 1981).

111. United States v. Marzano, 537 F.2d 257, 270–71 (7th Cir. 1976); Stonehill v. United States, 405 F.2d 738, 749–50 (9th Cir. 1968) (Browning, J., dissenting), *cert. denied*, 395 U.S. 960 (1969).

ing services" and not immediately receiving intercepted communications.[112]

All circuits, however, usually find joint ventures when the activity stretches beyond mere participation. The Ninth Circuit found a joint venture when DEA agents informed Philippines Narcotics Command of a suspect shipment headed to their ports, triggering Philippine authorities' initiation of wiretaps and intercepts. In this investigation, the DEA agents participated in the daily translation, decoding an analysis of intercepted transmissions. Seized evidence was treated as meant for the United States only, and the DEA called it a "joint investigation."[113] More recently, the Ninth Circuit found a joint venture when U.S. law enforcement requested the Danish police to place wiretaps, information obtained was immediately forwarded to U.S. law enforcement and the United States provided an interpreter throughout surveillance.[114] When foreign police conduct a search where one purpose among others is to convey evidence to the U.S. police, courts generally do not find a joint venture and instead admit the evidence.[115] Generally, if the foreign police know of the U.S. authorities' desire for the evidence because the United States suggested the investigation, judges still do not exclude the evidence when the search falls short of fourth amendment standards.[116] Under most cir-

112. United States v. Ferguson, 508 F. Supp. 2d 1, 5–6 (D.D.C. 2007).

113. United States v. Peterson, 812 F.2d 486, 490 (9th Cir. 1987).

114. United States v. Barona, 56 F.3d 1087, 1094 (9th Cir. 1995); *see also* Powell v. Zuckert, 366 F.2d 634 (D.C. Cir. 1966).

115. Johnson v. United States, 207 F.2d 314, 321 (5th Cir. 1953) (finding evidence obtained through a search of the defendant's hotel room by Cuban police admissible, even though Cuban police conducted search in order to help the Miami police obtain evidence in question and take defendant into custody, and they lacked consent necessary to meet fourth amendment standards).

116. *See* United States v. Behety, 32 F.3d 503, 510 (11th Cir. 1994) (declining to apply fourth amendment exclusionary rule to evidence obtained by the Guatemalan Navy, although a DEA agent initially provided Guatemalan military intelligence with information that led to the search and seizure of a U.S. vessel and contraband located therein); United States v. Maturo, 982 F.2d 57, 60 (2d Cir. 1992) (finding evidence admissible and no joint venture between the United States and Turkey where DEA requested information from Turkey, prompting Turkish wiretap that led to intercepts reviewed by U.S. authorities, on the grounds that the United States did not make the decision to tap phones); United States v. Hawkins, 661 F.2d 436, 456 (5th Cir. 1981) (finding no joint venture where Panamanian authorities searched a downed plane that the U.S. authorities said had drugs aboard); United States v. Rose, 570 F.2d 1358, 1362 (9th Cir. 1978); *Marzano*, 537 F.2d at 270.

cumstances, even when the U.S. authorities request or participate in a foreign search, courts will not find a joint venture.[117]

III. HOW TECHNOLOGY HAS ALTERED THE TEST FOR JOINT VENTURE

Though we live in a highly advanced technological time, the legal framework governing joint ventures is based on standards and guideposts used when coordination between different law enforcement entities was almost always physical rather than technological. In fact, most of the cases extending the silver platter doctrine and its joint venture exception to international investigations occurred in the 1970s, before the revolution in information and communications technology. In the twenty-first century, technology and the pervasive transnational terrorist threat have broadened the scope of the international silver platter doctrine, reduced the impact of its joint venture exception and consequently rendered the Fourth Amendment, in practice, virtually inapplicable to most transnational terrorism investigations. Rather than relying on deferential courts or the over-eager executive, Congress can best resurrect the fourth amendment stand-

117. *Behety*, 32 F.3d at 510 (declining to exclude evidence obtained through search of U.S. vessel by Guatemalan officials, even though DEA agent was present and videotaped the search); United States v. Rosenthal, 793 F.2d 1214, 1231 (11th Cir. 1986) (finding no joint venture where U.S. authorities were present at search and arrest at request of Colombian authorities); United States v. Benedict, 647 F.2d 928, 931 (9th Cir. 1981) (finding no joint venture where U.S. agents were called by Thai authorities who initiated the investigation, as the U.S. agents played only a "passive role"); United States v. Maher, 645 F.2d 780, 783 (9th Cir. 1981) (finding no joint venture because investigation was initiated and controlled by Canadian police, with only limited support from U.S. officials); Gov't of the Canal Zone v. Sierra, 594 F.2d 60, 72–73 (5th Cir. 1979) (finding evidence admissible where a foreign government initiated the search to enforce its own laws, even though U.S. agents were present and provided assistance); Stowe v. Devoy, 588 F.2d 336, 341–42 (2d Cir. 1978) (finding evidence admissible when obtained by Canadian authorities enforcing Canadian law, as the presence of U.S. agents during search alone was insufficient grounds for exclusion); *Marzano*, 537 F.2d at 270–71 (declining to exclude evidence obtained through a foreign police search and seizure, as FBI agents were present but played no active role in the interrogation, search or selection of evidence to seize); Stonehill v. United States, 405 F.2d 738, 743 (9th Cir. 1968) (finding no joint venture where IRS agent sent informant to accompany Philippines government official to select relevant documents from warehouse searched by foreign officers), *cert. denied*, 395 U.S. 960 (1969); Birdsell v. United States, 346 F.2d 775, 782 (5th Cir. 1965) (declining to exclude evidence where Texas sheriff in Mexico acted as translator during search); State v. Barajas, 238 N.W.2d 913, 915–16 (Neb. 1976) (finding no joint venture where U.S. sheriff requested that Mexican police search residence in Mexico for weapon used in homicide).

ards abroad by articulating statutory rules governing transnational investigations.

A. Applying an Antiquated Legal Foundation to Modern Threats

The joint venture doctrine derives from early twentieth-century rules governing how federal prosecutors could use evidence collected by state authorities. Before the Supreme Court applied the exclusionary rule against the states in 1961,[118] fourth amendment requirements for searches and seizures, which carefully circumscribed and limited the scope of federal investigations, did not bind state officials. Nevertheless, the Supreme Court allowed federal prosecutors to present evidence gathered by state police that did not meet fourth amendment standards.[119] In other words, under what became known as the state silver platter doctrine, a federal court could admit the fruits of searches conducted by state law enforcement, even though the court would exclude that evidence if it had been gathered by federal authorities.[120]

As coordination between federal and state law enforcement in criminal investigations expanded, some worried that federal authorities would circumvent constitutional restrictions by appointing state officials to conduct unconstitutional searches and presenting that evidence in court. To prevent such constitutional evasion, a joint venture exception extended the exclusionary rule to evidence gathered from cooperative searches and seizures that fell short of constitutional standards.[121] Courts in the early twentieth century interpreted the joint venture exception broadly, applying the exclusionary rule even if federal authorities were just ancillary to the search, as long as the court found federal participation or a federal purpose in the state ac-

118. Mapp v. Ohio, 367 U.S. 643, 655 (1961).

119. Gambino v. United States, 275 U.S. 310, 317 (1927); Byars v. United States, 273 U.S. 28, 33 (1927).

120. Nat'l Safe Deposit Co. v. Stead, 232 U.S. 58, 71 (1914) (holding that the Constitution does not prohibit unreasonable searches by state authority); Weeks v. United States, 232 U.S. 383, 398 (1914) (refusing to extend the exclusionary rule to state seizures); Adams v. New York, 192 U.S. 585, 594 (1904) (refusing to inquire into how otherwise-admissible evidence was acquired).

121. Irvin B. Nathan & Christopher D. Man, *Coordinated Criminal Investigations Between the United States and Foreign Governments and Their Implications for American Constitutional Rights*, 42 VA. J. INT'L L. 821, 822–23 (2002).

tion.[122] In 1941, Justice Frankfurter distinguished between federal and state searches in one of the more famous articulations of the state silver platter doctrine:[123]

> The crux of that doctrine is that a search is a search by a federal official if he had a hand in it; it is not a search by a federal official if evidence secured by state authorities is turned over to federal authorities on a silver platter. The decisive factor in determining the applicability of the [silver platter doctrine] is the actuality of a share by a federal official in the total enterprise of securing and selecting evidence by other than sanctioned means.[124]

Though the state silver platter doctrine was overruled by *Elkins v. United States* in 1960,[125] lower courts resurrected Frankfurter's articulation and applied to it evidence unlawfully seized by foreign officials in transnational law enforcement investigations.[126]

While some scholars argue that the test for federal involvement in foreign searches should replicate that articulated in *Lustig*,[127] courts have interpreted the joint venture exception to the international silver platter doctrine much more narrowly than the state doctrine. For instance, the state doctrine finds a joint venture when a federal officer is summoned to the scene of a state search before all the evi-

122. *Id.* at 827; *see also Gambino*, 275 U.S. at 310 (finding a joint venture even when federal officers did not participate in the search or know it occurred, because it was conducted solely for federal authorities); *Byars*, 273 U.S. at 32 (finding a joint venture when state officers searched a house alongside a federal officers with a warrant failing fourth amendment standards; cautioning other courts to "be vigilant to scrutinize the attendant facts with an eye to detect and a hand to prevent violations of the Constitution by circuitous and indirect methods").

123. Lustig v. United States, 338 U.S. 74 (1949).

124. *Id.* at 78–79.

125. 364 U.S. 206, 208 (1960).

126. Stonehill v. United States, 405 F.2d 738, 743 (9th Cir. 1968), *cert. denied*, 395 U.S. 960 (1969); *see also* Kaplan, *supra* note 87, at 503–05; Robert L. King, Note, *The International Silver Platter and the "Shocks the Conscience" Test: U.S. Law*, 67 WASH. U. L.Q. 489, 493–94 (1989).

127. *See* W.J.A., *supra* note 92, at 282–83 ("Since foreign officers occupy the same position as did state officers during the silver platter era prior to 1960, and since searches by foreign officers present problems similar to those created by state searches during this era, the standards developed and applied to state searches prior to 1960, at least logically, should apply equally to searches by foreign officers.").

dence was seized,[128] but similar federal presence during a foreign search is insufficient to trigger fourth amendment protection.[129] These distinctions hinge on the concerns over federal officers outsourcing questionable searches to state officers in order to circumvent constitutional restrictions.[130] Unlike domestic searches, in a foreign country "the Federal officer ordinarily has no authority to conduct searches and seizures on his own initiative; he must depend on cooperation from the local authorities."[131] Thus, in the context of transnational investigations, there may be less fear that federal authorities will manipulate their foreign counterparts to evade constitutional requirements.

Despite these differences, the joint venture exception to the international silver platter doctrine has its analytical and legal foundation in the state doctrine, which developed almost one hundred years ago—long before the internet and the modern globalized economy. The world has dramatically changed since the first articulation of the joint venture exception in the early twentieth century: the United States is an international superpower; technology and globalization allow events across the world to have instant domestic ramifications; instead of conventional enemies, the United States faces amorphous borderless terrorist organizations that use technology to camouflage their activities and develop modern deadly weapons; globalization has made international coordination between law enforcement more common, while the rise of transnational terrorism has made this collaboration imperative; the technology used in cooperative transnational investigations eclipses any tools imagined in Justice Frankfurter's day; and courts struggle to apply an antiquated legal foundation to novel threats. As explained below, this struggle weakens the Fourth Amendment in transnational terrorism investigations by expanding the international silver platter doctrine and limiting its joint venture exception.

128. *Lustig*, 338 U.S. at 79.

129. United States v. Behety, 32 F.3d 503, 511 (11th Cir. 1994) (finding that a DEA agent's presence during a search of U.S. vessel by Guatemala officials not enough of a joint venture to trigger exclusion).

130. *See* Byars v. United States, 273 U.S. 28, 32 (1927).

131. W.J.A., *supra* note 92, at 312; *see, e.g.*, United States v. Morrow, 537 F.2d 120, 139 (5th Cir. 1976).

B. Technology Changes How Searches Are Conducted and Alters Factors Defining Joint Venture

Technological progress, the rise of terrorism and increased international coordination have transformed the landscape surrounding the international silver platter doctrine and how its joint venture exception is applied.[132] International coordination creates more potential opportunities for joint ventures, but technology actually allows many collaborative actions to circumvent the requirements of a joint venture. These twenty-first century changes increase the use of the international silver platter doctrine, but minimize application of its joint venture exception. As a whole, applying the antiquated legal calculus in this novel context narrows the range of activities encompassed in the joint venture exception and, in turn, allows more evidence gathered in unreasonable foreign searches to be presented in U.S. federal court. Notably, this transformation undermines the original intent of the joint venture exception—preserving the Fourth Amendment's application to officials overseas. Instead, with changed circumstances rendering the old standards moot, technological and remote coordination allow officers to clear fourth amendment hurdles easily and present the products of unreasonable collaborative foreign searches in court.

Technology and increased international interconnectivity expand the application and alter the scope and the meaning of the international silver platter doctrine in three key ways: first, these changes broaden the range of, and create more opportunities for, transnational collaboration that could be considered joint ventures, thereby amplifying the invocation of the international silver platter doctrine; second, by distorting the meaning of the three key phrases used by the circuits to define joint ventures, new circumstances narrow the scope of the joint venture exception; and third, technology and increased collaboration transform activity previously encompassed within the doctrine to something less than joint venture.

132. *C.f.* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 804 (2004) (examining technology's impact on fourth amendment law and urging a flexible, broad interpretation).

1. Technology and Globalization Create More Opportunities for Joint Venture Analysis

Technology and globalization vastly enlarge the range of activities subject to joint venture analysis by (1) increasing the likelihood of targeting a U.S. person and thus boosting the application of the Fourth Amendment to foreign searches, (2) amplifying the opportunities for cooperation on foreign searches and (3) expanding methods of international collaboration. As a result, federal courts will likely face more evidentiary challenges on the international silver platter doctrine, with prosecutors urging the admission of products of "foreign searches," while defense attorneys object on fourth amendment grounds, labeling the search a "joint venture."

First, technology and globalization increase the probability that terrorist investigations target U.S. persons abroad and that the government later attempts to present the products of that foreign search at trial. The global nature of terrorism and the technological advances increase the risk of American involvement in terrorist activities. FBI Director Robert Mueller notes,

> [A]s the Internet continues to shape the way American society engages in so much of our daily lives and routines, so too has it had a profound impact on the radicalization dynamic. The Internet has expanded as a platform for spreading extremist propaganda, a tool for online recruiting, and a medium for social networking with like-minded violent extremists, all of which may be contributing to the pronounced state of radicalization inside the United States.[133]

The FBI anticipates that Al-Qaeda will recruit more U.S. persons to launch attacks, which in turn means that more search targets will be protected by the Fourth Amendment.[134] The FBI cites an increased number of U.S. persons traveling abroad to train in terrorist camps. For example, since at least twenty-four Americans have traveled to Somalia to train and fight on behalf of Al-Shabaab in recent

133. *Nine Years After 9/11: Confronting the Terrorist Threat to the Homeland: Hearing Before the S. Comm. on Homeland Sec. and Governmental Affairs*, 111th Cong. (2010) (statement of Robert S. Mueller III, Director, Federal Bureau of Investigation) [hereinafter *Nine Years After 9/11*], *available at* http://hsgac.senate.gov/public/index.cfm?FuseAction=Files.View&FileStore_id=9cda2966-30ed-48e2-b3a9-7d40f0b617e5.

134. *Id.*

years,[135] investigations into that organization may target and later prosecute U.S. citizens. If a joint venture is found, fruits of "unreasonable" searches may be suppressed.

Second, the rise of transnational terrorism and the globalized economy have forced the United States to coordinate with foreign law authorities more extensively than ever before, providing far more opportunities for cooperative searches and seizures abroad. As terrorist organizations thrive and undermine local law enforcement by collaborating across borders, the United States must join forces with international partners to combat the threat effectively. For example, during the early years of the Iraq War, when conventional communication lines were cut, resistance groups used websites to post maps and safe-house locations to assist prospective insurgents from Saudi Arabia or Europe traveling to Iraq to join the fight.[136] Iraqi insurgents also used the internet to spread successful military tactics, like designs for advanced remote-triggered Improvised Explosive Devices (IEDs), to other terrorist groups in Afghanistan and Thailand.[137] Since terrorist groups are borderless, counterterrorism efforts also must be borderless to succeed: "Intelligence-driven investigations also require a unity of effort with our partners overseas. Global cooperation is necessary to combat terrorism."[138] Currently, the United States has thousands of federal agents stationed abroad with the consent of local law enforcement authorities,[139] working alongside local authorities to collect evidence for domestic prosecutions.[140] The

135. *Id.*

136. Brachman, *supra* note 8, at 154.

137. Thailand police attribute the IED modifications in part to the distribution of jihadi training manuals through the internet and CD-ROMs. *See id.*

138. *Nine Years After 9/11*, *supra* note 133 ("By sharing financial resources, training, tactical and operational expertise, and recruits, these groups have been able to withstand significant counterterrorism pressure from United States, coalition, and local government forces.").

139. *See* Mermelstein, *supra* note 83, at 34. The FBI has legal attachés in seventy-five foreign cities and over 200 countries, territories and islands. *Legal Attaché Offices*, FEDERAL BUREAU OF INVESTIGATION, http://www.fbi.gov/contact/legat/legat.htm (last visited Jan. 4, 2011). The DEA has eighty-two foreign offices in sixty-two countries. *DEA Office Locations*, U.S. DRUG ENFORCEMENT ADMINISTRATION, http://www.justice.gov/dea/agency/domestic.htm (last visited Jan 31, 2011).

140. The agents' authority to operate in the host country is limited by each nation's consent. *See* Mermelstein, *supra* note 83, at 34; *see also* ETHAN NADELMAN, COPS ACROSS BORDERS: THE INTERNATIONALIZATION OF U.S. CRIMINAL LAW ENFORCEMENT 181 (1993); *Nine Years After 9/11*, supra note 133 ("Through more than 60 legal attaché offices around

sheer presence and number of these agents abroad is another illustration of how frequently the United States works with foreign partners, which in turn reveals the unprecedented opportunities for joint venture analysis.

Collaboration almost always occurs in the terrorism context, because a single terrorist act cannot be considered a discrete incident. Instead, authorities must look holistically to threats abroad, examining how the target organization fits into a larger network of extremists.[141] Since extremist organizations have global roots and connections, information gathered by one police force could prove essential for another law enforcement entity. For example, after arresting Umar Farouk Abdulmatallab for the 2009 Christmas Day bombing attempt, the FBI established a "Yemen fusion cell to coordinate intelligence and counterterrorism assets in response to al Qaeda in the Arabian Peninsula's (AQAP's) threat to the United States homeland and United States interests overseas."[142] The FBI gained "critical" information and shared it with its "partners in the intelligence and law enforcement communities."[143] Similarly, after arresting naturalized U.S. citizen Faisal Shahzad for the attempted Times Square bombing of May 2010,[144] the United States "expeditiously" shared the "voluminous and significant" intelligence gathered from the investigation with domestic and foreign partners.[145] Further, in October 2009, U.S. law enforcement arrested U.S. citizen David Headley in Chicago for involvement in both a terrorist plot against a Danish newspaper and the 2008 attacks in Mumbai.[146] In U.S. court, Head-

---

the world, the FBI has strengthened relationships with our international partners and expanded our global reach.").

141. *Nine Years After 9/11*, *supra* note 133 ("Addressing our most critical threats requires a holistic picture and understanding of the threat environment at home and abroad.").

142. *Id.*

143. *Id.*

144. *Id.*

145. *Id.*

146. *Id.*; *see also* Press Release, Dept. of Justice, Chicago Resident David Coleman Headley Pleads Guilty to Role in India and Denmark Terrorism Conspiracies (Mar. 18, 2010), http://chicago.fbi.gov/dojpressrel/pressrel10/cg031810.htm. Headley traveled to India at least five times to scout potential targets for attacks by Lashkar-e-Taiba (a militant Pakistani group), recorded each target's GPS coordinates and videotaped each location. The information he provided was used to execute the 2008 Mumbai attacks. Carrie Johnson, *U.S. Citizen David Coleman Headley Admits Role in Mumbai Attacks*, WASH. POST, Mar. 19, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/03/18/AR2010031805407.html; *Pakistani American Posed as Jew To Case Mumbai Chabad*, JTA, Nov. 15, 2009,

ley pled guilty in March 2010 to conspiring to bomb targets in Mumbai, providing material support to Lashkar-e-Taiba and aiding and abetting murder of U.S. citizens in the 2008 Mumbai attacks.[147] At the same time, India's National Investigation Agency (NIA) registered a case against Headley.[148] U.S. authorities reportedly shared "significant information" with Indian authorities on the case,[149] provided real time access to information gathered from Headley,[150] and even facilitated NIA's June 2010 interrogation of Headley in the United States.[151] Because information sharing is a crucial counterterrorism tool, crushing the terrorism threat in essence requires a joint venture amongst all law enforcement internationally. The counterterrorism battle hinges on flourishing relationships with liaison partners—thus creating unprecedented opportunities for the application of the international silver platter doctrine and its joint venture exception.

Third, the changed nature of technology itself has revolutionized the techniques countries employ to coordinate counterterrorism efforts, thereby further expanding the types of activities that could be considered joint ventures. Compared to the 1960s and 1970s, when the international silver platter doctrine was first applied, current transnational communications are unprecedented, with millions of

---

http://jta.org/news/article/2009/11/15/1009195/us-pakistani-posed-as-jew-to-case-mumbai-chabad; Praveen Swami, *American Jihadist Helped Plan 26/11 Carnage*, HINDU (India), Dec. 8, 2009, http://beta.thehindu.com/news/national/article61652.ece.

147. Johnson, *supra* note 146; *Mumbai Terror Suspect Pleads Guilty*, CNN, Mar. 18, 2010, http://news.blogs.cnn.com/2010/03/18/mumbai-terror-suspect-pleads-guilty/; Mike Robinson, *Terror Suspect Admits Scouting for Mumbai Massacre*, ABC NEWS, Mar. 18, 2010, http://abcnews.go.com/US/wireStory?id=10132245; *Terror Suspect Likely To Change Plea*, N.Y. TIMES, Mar. 16, 2010, http://www.nytimes.com/2010/03/17/us/17plea.html.

148. Vinay Kumar, *NIA Registers Case Against Headley, Rana,* HINDU (India), Nov. 13, 2009, http://www.hindu.com/2009/11/13/stories/2009111305220100.htm.

149. *India Plans To Try Chicago Man for Mumbai Attacks*, REUTERS, Dec. 8, 2009, http://www.reuters.com/article/2009/12/08/us-india-fbi-mumbai-idUSTRE5B72I620091208; *see* Plea Agreement, United States v. Headley, No. 09 CR 830-3 (N.D. Ill. Mar. 18, 2010), *available at* http://beta.thehindu.com/news/international/article258037.ece; Steve Herman, *U.S. Promises India "Full Access" to Mumbai Attack Planner*, VOICE OF AMERICA, Mar. 20, 2010, http://www1.voanews.com/english/news/asia/88719992.html; Nigam Prusty, *India Wants To Question U.S. Man on Mumbai Attack*, REUTERS, Mar. 19, 2010, http://www.reuters.com/article/idUSTRE62I1MC20100319.

150. *Access to Headley Being Worked Out at the Highest Level: Roemer*, HINDU (India), Apr. 19, 2010, http://beta.thehindu.com/news/national/article405231.ece.

151. *India Granted Access to Headley*, INDIAN EXPRESS, June 5, 2010, http://www.indianexpress.com/news/india-granted-access-to-headley/629839/1.

phone calls and emails crossing international boundaries each day.[152] Interception and information-sharing technology enable countries to investigate terrorism cells using novel methods. For example, U.S. and Indian counterterrorism experts proposed new techniques for improving Indo-U.S. counterterrorism cooperation; the techniques proposed included the adoption of joint ground-to-space surveillance systems using sensors, as well as placing information-gathering systems consisting of biomaterials, nanomaterials, high-resolution thermal vision systems and body-embedded microelectromechanical systems (MEMS) on bridges, highways and nuclear platforms.[153] Both the United States and India could remotely monitor data collected from space-based surveillance systems and share analyzed information to avoid attack and track terrorists.[154] This type of cooperation has unprecedented fourth amendment implications, especially for the international silver platter doctrine and its joint venture exception.[155]

The expanded opportunities for finding joint ventures are particularly clear in the cyberwarfare context. Suppose the United States assists a foreign government by using cyberwarfare techniques that would be otherwise unavailable to that nation. For example, the United States has actively invested in tracking technologies to pin down instigators of cyber attacks, like the Air Force's "Proactive Botnet Defense Technology" that can locate the source of the hacking and manipulate that computer system.[156] Further suppose that the Philippines suffers a cyber attack that jams and disables websites of the government, banks, newspapers and the media. The United States seeks to aid its ally by using the program to identify the location of the hacker's computer. Information gathered allows Philippine authorities to remotely access the contents of the perpetrator's

152. *See* Nelson, *supra* note 93, at 349.

153. T.G.K Murthy & John Holdren, *Discussion of Indo-U.S. Cooperation*, *in* SCIENCE AND TECHNOLOGY TO COUNTER TERRORISM: PROCEEDINGS OF AN INDO-U.S. WORKSHOP 151 (Roddam Narasimha et al. eds., 2007), *available at* http://books.nap.edu/openbook.php?record_id=11848&page=151.

154. *Id.* at 151–52.

155. Information sharing between the intelligence community and their foreign counterparts through formal or non-binding agreements also creates more opportunities for joint venture analysis. In July 2010, the Department of State and Terrorist Screening Center made non-binding arrangements or formal agreements with eighteen foreign partners, facilitating the reciprocal exchange of terrorism screening information. *Sharing with International Partners*, INFORMATION SHARING ENVIRONMENT, http://www.ise.gov/Pages/SIP.aspx (last visited Mar. 18, 2011).

156. Berry, *supra* note 12, at 9.

computer and discover that he is a member of Jemaah Islamiyah, a militant Southeast Asian Islamic terrorist organization. The search also reveals that the hacker is a naturalized U.S. citizen suspected of planning attacks against U.S. tourists abroad. Could the United States present this evidence against the perpetrator in a future criminal prosecution in federal court? Under joint venture analysis, would the United States' provision of technical assistance during a Philippine national security crisis be considered mere assistance? Or was U.S. aid substantial enough to constitute a joint venture, considering that country would otherwise lack access to those technologies? Increased international coordination through novel technological resources creates more opportunities for joint venture analysis, but also makes the application of the parameters ambiguous, leaving wiggle room in fourth amendment joint venture doctrine.

Further, when investigating a cyberterrorism attack, the unique nature of the threat modifies the joint venture analysis. More often than not, authorities will not know where the hacker is from or who he is. For example, when the U.S. Air Force laboratory computer system in New York was attacked in March of 1994, authorities traced the attacker's ISP to Seattle, Washington, but then lost the trace. Over 150 attacks on the laboratory followed from 100 different points of origin, with the hacker manipulating his computer so that the attacks were traced to unrelated locations.[157] When authorities cannot clearly identify the threat because it is hidden behind the shield of technology, it is not clear whether interception by a foreign government significantly helped foreign police or was done solely for the benefit of the U.S. authorities, and thus it is not clear whether the exclusionary rule applies. The next Section illustrates how the globalized and technical nature of the threat makes traditional boundaries uncertain, and attempts to clarify the application of old joint venture parameters to new fact patterns.

2. The Joint Venture Parameters in the Twenty-First Century

The three joint venture standards articulated by the circuits—which require (1) substantial participation of a U.S. official, (2) an agency relationship between foreign authorities and the federal government and/or (3) intentional constitutional evasion by U.S. authorities—have new and more limited meanings in the twenty-first

157. Authorities did not identify the perpetrator, a sixteen-year-old from the United Kingdom who was assisted by a twenty-two-year-old Israeli, until he boasted of his exploits. *Id.* at 3.

century. These meanings narrow the range of activities encompassed in the joint venture exception and, in turn, allow more evidence gathered in unreasonable foreign searches to be presented in U.S. federal court.

a. Parameter One: Substantiality of U.S. Involvement

Under the first standard, many circuits define joint venture, in part, as a search or seizure involving substantial participation of a U.S. official.[158] Technological advances have transformed the circumstances that were once considered substantial enough to trigger the Fourth Amendment. Joint venture analysis thirty years ago relied heavily on the physical presence of U.S. agents in the foreign searches to determine the substantiality of their participation, and now technology renders many of these parameters moot.[159] In fact, increased remote collaboration through the internet and satellites has pushed interactions that were once deemed substantial participation into mere participation Through new tools like remote search technology or satellite sensors, government officials may not be present at all for the search, but through technology may remotely facilitate or control much of the investigation. For example, law enforcement in the United States could assist a foreign terrorist investigation by "withdraw[ing] money from terrorist bank accounts, impersonat[ing] a terrorist's voice on the telephone, disrupt[ing] voice/data communications completely, and disrupt[ing] GPS signals used by a terrorist's navigation equipment."[160] Often, when an official located in the United States contributes to a foreign search through these methods, the technology may conceal the significance of U.S. participation. In

158. United States v. Barona, 56 F.3d 1087, 1091 (9th Cir. 1995).

159. A recent case shows how the court still focuses on physicality in determining the "substantiality" of U.S. involvement with foreign searches. In *United States v. Stokes*, 710 F. Supp. 2d 689 (N.D. Ill. 2009), the district court found a joint venture when U.S. and Thai agents searched the home of a U.S. citizen living in Thailand and seized property. *Id.* at 699. The court noted that Thai authorities directed the search, but U.S. authorities were substantially involved in the search and prior investigation. *Id.* ICE officials requested the search, worked with Thai authorities to identify the target and plan the search and physically conducted the search. *Id.* Like the early silver platter doctrine cases, the court focused on the physical involvement of the U.S. authorities, noting that an ICE agent was the first to speak to the defendant, entered the house first and seized the first camera. *Id.* The court also stressed that all items seized by the Thai police were turned over to ICE agents. *Id.* Thus, the court found a joint venture and applied fourth amendment requirements to the search. *Id.*

160. Lin et al., *supra* note 6, at 155.

the past, physical presence and co-location of personnel could be easily documented and observed, but new forms of international collaboration are less visible. The cyber or non-physical aspect of the action may make U.S. participation seem less substantial than it really is, thereby pushing searches once considered joint ventures in the purely physical realm into primarily foreign searches given special status under the international silver platter doctrine.

Similarly, with counterterrorism initiatives increasing the flow of information between countries, under the joint venture analysis information technology may cloud the substantiality of American participation. For example, the Information Sharing Environment (ISE)[161] facilitates the exchange of terrorism information, including intelligence and law enforcement data, between the government and foreign actors. This new type of technological coordination proves a valuable tool in transnational criminal investigations,[162] with some attributing recent successful targeting and arrests in Pakistan, France and North Africa to increased information sharing between the United States and European allies.[163] Collaboration can form the pivotal component of a foreign terrorist investigation, but will not likely be deemed substantial enough to establish a joint venture because it lacks physical involvement. Thus, the joint venture doctrine's failure to account for technological changes when determining the substantiality of U.S. involvement results in new resources camouflaging truly substantial interaction as mere participation.[164]

---

161. Intelligence Reform and Terrorism Prevention Act, Pub. L. No. 108-458, 118 Stat. 3638 (2004) (laying out the ISE in section 1016); INFORMATION SHARING ENVIRONMENT, http://www.ise.gov/default.aspx.

162. See CARAFANO & WEITZ, *supra* note 9, at 4, for methods to enhance cyber security.

163. Marc Ambinder, *Countries Sharing Intel Key to Terrorism Arrests*, ATLANTIC, Oct. 5, 2010, http://www.theatlantic.com/politics/archive/2010/10/countries-sharing-intel-key-to-terrorism-arrests/64091. For example, intelligence gathered by France and passed on to American intelligence agencies reportedly revealed a plotted attack by a German terrorist cell, which in turn allegedly led to an American military strike against suspected terrorists in North Waziristan. The intelligence sharing goes both ways, with news sources reporting that the United States passed information to European allies about increased terrorist activity in North Africa (including specific jihadi training camps) as part of al-Qaeda in Islamic Maghreb, which France allegedly used to target suspected terrorists. *Id.*

164. Many recent cases address terrorism and the Fifth Amendment's silver platter doctrine and joint venture exception, which is analogous to the Fourth Amendment's exception (testimonial statements elicited by foreign police without proper Miranda warnings must be suppressed, if the United States is in a joint venture with foreign officials). In *United States v. Marzook*, 435 F. Supp. 2d 708, 759 (N.D. Ill. 2006), when the prosecution attempted to introduce the defendant's statements to Israeli authorities, the district court found no joint venture, holding that the United States did not actively

b. Parameter Two: Acting as Agents of the U.S. Government

Second, some circuits apply fourth amendment protections when foreign authorities act as agents of the federal government. This standard has new meaning in the twenty-first century because of remote involvement by U.S. authorities and the challenge of isolating the driving motivation behind the search. Generally, if U.S. officials are present at, request and participate in the search, and if foreign officials act solely at the behest of the U.S. officials, then the Fourth Amendment applies.[165] The ability of U.S. officials to coordinate with foreign investigators through communication technology, without any physical presence at the search, may undercut the agency parameter's application to many forms of transnational collaboration. While traditionally it may have been difficult to prove whether U.S. personnel drove the investigation, modern U.S. communication to foreign counterparts solely through satellite transmissions or electronic databases amplifies this challenge. In order to preserve this standard's force, courts must recognize the technological ability of the United States *remotely* to be present at, direct and participate in a foreign search.

More importantly, the pervasiveness of transnational terrorism also changes the meaning of the "agency" parameter. Since ter-

---

participate in questioning because there were no investigative contacts, communications, requests or instructions between the FBI and Israeli police, and no indication that Israelis were asking certain questions on the United States's behalf. The court also found that U.S. agents did not use foreign officials to evade constitutional requirements because there was no evidence indicating a pending investigation by the United States against the defendant at the time of the statement. *Id.* In *United States v. Abu Ali*, 528 F.3d 210, 227 (4th Cir. 2008), the prosecution attempted to present statements of the defendant, a citizen charged with assisting a designated terrorist organization, gathered from a 2003 Saudi Arabia interrogation for suspected involvement in the 2003 Riyadh bombings. The court held the statements were admissible, even though Miranda warnings were not given, because the Saudis controlled the interrogation, only allowing secret observation by American officials and six pre-approved U.S. questions. The court stressed that Saudi officials arrested the defendant independently based on their own information and interest in investigating the Riyadh bombings. Because of this split motive and the fact that the United States lacked investigative control and authority, there was no joint venture. Notably, in the lower court decision, *United States v. Abu Ali*, 395 F. Supp. 2d 338, 341 (E.D. Va. 2005), the defendant also moved to suppress evidence from a search of his dorm room in Medina, Saudi Arabia. The district court held that the search was not a joint venture, and that the search products were not protected by the Fourth Amendment. *Id.* at 381–83; *see also* Stephen I. Vladeck, *Terrorism Trials and the Article III Courts After* Abu Ali, 88 TEX. L. REV. 1501 (2010) (analyzing the evidentiary issues faced by the Fourth Circuit).

165. United States v. Behety, 32 F.3d 503, 510 (11th Cir. 1994).

rorism poses a threat to all countries, it is extraordinarily rare for foreign officials to search or seize "solely" on behalf of the United States. Indeed, existing silver platter case law repeatedly states that if foreign authorities act for other motives as well, a joint venture is usually not found.[166] The borderless nature and accompanying permeating globalized threat of terrorism operations, consequently, render the "acting as agents" definition a dead letter in the context of counterterrorism searches and seizures.

The investigation surrounding the July 2010 bombings in Uganda's capital of Kampala during the World Cup final illustrates the difficulty of isolating primary motives.[167] Responding to a request by Ugandan leaders, the FBI New York Joint Terrorism Task Force (JTTF) sent agents, analysts and forensic experts to assist the Ugandan investigation. U.S. officials helped collect evidence at the bomb scene, conducted explosive analysis and reconstructed photos of two suspected bombers.[168] The investigation was a truly collaborative effort involving the U.S embassy, the FBI, the British High Commission, the New Scotland Yard, Interpol and other nations.[169] The FBI Special Agent in charge suggested dual motives for U.S. involvement, noting that "[t]he United States has been victim to serious terrorist attacks and we have learned that partnerships, such as the one we have with Uganda are critical in investigating and preventing these attacks."[170] Notably, some local newspapers suggested that the FBI "hijacked" the investigation and "supervis[ed] Uganda and Kenya police to make a clean sweep of all people suspected to be members of East Africa's Al Qaeda cells."[171] The Ugandan reporter al-

166. *See* cases cited *supra* notes 115–17.

167. Jim Kouri, *FBI Hunts for Terrorist Bombers in Africa*, EXAMINER (July 22, 2010) http://www.examiner.com/public-safety-in-national/fbi-hunts-for-terrorist-bombers-africa. At least seventy-four people were killed in the attacks. *FBI Team Helping with Bomb Investigation in Uganda*, CNN, July 12, 2010, http://articles.cnn.com/2010-07-12/us/uganda.bombing.white.house_1_bomb-investigation-fbi-team-uganda-government?_s=PM:US. The Somali Islamic militant group Al-Shabaab claimed responsibility for the attacks. Kouri, *supra*.

168. *FBI Team Helping with Bomb Investigation in Uganda*, *supra* note 167; *see also* Kouri, *supra* note 167.

169. U.S. investigators were "appreciative of the complete support from [the Ugandan Inspector General of Police] and the police force as we work[ed] together to support their investigation." Kouri, *supra* note 167.

170. *Id.*

171. One newspaper reports that thirteen Kenyans were transported to and detained in Uganda. Julius Barigaba, *FBI, Police Yet To Link Kenyans to Kampala Blasts*, THE E. AFRICAN (KENYA), Oct. 4, 2010, http://allafrica.com/stories/201010040875.html.

leges that the FBI's motives were not limited to investigating the Kampala bombings but also extended to the disruption of terrorist rings throughout East Africa.[172] In response, the U.S. embassy denied that "any agency of the United States government, was present, participated or directed in any way the arrest, detention and questioning of [the Kenyan suspects]," maintaining that the FBI's role is to investigate crimes against U.S. citizens anywhere and noting that the Kampala attacks killed an American and injured at least three other Americans.[173] The multiple conflicting motives in the Ugandan investigation exist in most transnational collaborations. Nevertheless, even though U.S. assistance may have been driven by broader counterterrorism goals, Ugandan authorities cannot be found to be acting as agents of the U.S under the joint venture standards since they investigated in order to discover and prosecute the perpetrators themselves.

In fact, a recent district court found no joint venture when U.S. authorities played a much larger role in directing and initiating the investigation. In *United States v. Defreitas*, the defendant faced charges for conspiring to attack John F. Kennedy International Airport by exploding fuel storage tanks.[174] The investigation into the conspiracy began in early 2006, and on June 1, 2007, a U.S. magistrate judge issued an arrest warrant for four co-conspirators, leading to U.S. citizen Defreitas's arrest in New York.[175] On June 6, 2007, Guyanese officers searched Defreitas's residence in Georgetown, Guyana, pursuant to a warrant for suspected possession of firearms or explosives.[176] The next day Guyanese police conducted a second

172. The reporter asserts that the U.S. investigators used Ugandan and Kenyan law enforcement agencies to carry out renditions on suspected terrorists. *Id.* Newspapers also reported that FBI agents extended the investigation to Somali oil dealers in East Africa because of their link to the Ugandan July 2010 bombings. Some argue that the United States broadened the scope of the investigation to meet broader counterterrorism objectives by thwarting Al-Shabaab members' use of the oil tankers to enter other countries. Dalton Wanyera, *FBI Investigating Somali Oil Dealers in East Africa*, UGANDA EYE, Aug. 3, 2010, http://saraarmedia.com/blog/2010/08/03/fbi-investigating-somali-oil-dealers-in-east-africa.

173. Barigaba, *supra* note 171, at 3.

174. United States v. Defreitas, 701 F. Supp. 2d 297, 300 (E.D.N.Y. 2010).

175. *Id.* at 300–01. Local officers in Trinidad and Tobago arrested co-conspirators Abdul Kadir and Kareen Ibrahim, Guyanese citizens, pursuant to provisional arrest warrants based on the U.S. warrant, and extradited them to New York on August 6, 2007. Crucially, since the Fourth Amendment is not applicable to non-U.S. citizens with no voluntary connections to the U.S, there is no exclusionary remedy for searches and seizures against Defreitas's co-defendants in Trinidad and Tobago and Guyana.

176. *Id.* at 301.

search with FBI agents and, pursuant to a second Guyanese warrant, seized passports, diaries, audio tapes, floppy disks and two computer hard drives.[177] The Guyanese officials turned over the hard drives to the U.S. agents who shipped them to New York, where they acquired a second warrant to search the hard drives.[178] Defreitas moved to suppress evidence gathered by officials abroad, arguing that U.S. participation made the searches joint ventures.[179] The court disagreed, holding that foreign officials were not "acting as [U.S.] agents" even though the search was motivated by the U.S. investigation, stressing that U.S. authorities were not involved in decisions to execute the Trinidad searches or to search the suspect's house in Guyana.[180]

c. Parameter Three: Evading the Constitution

Finally, some circuits include an "evading the Constitution" parameter in the joint venture test, extending fourth amendment protections if U.S. officials use the foreign government to circumvent the Constitution.[181] While technological advances at first glance do not seem to greatly alter this test because it is always applied in conjunction with the substantiality or agency parameters, the same concerns articulated above undermine its force and effectiveness. Terrorism investigations, however, stand on different legal footing from traditional criminal investigations. Unlike traditional crime, terrorism threatens national security, implicates foreign relationships and is part of a broader war on terrorism. Arguably, the President and Congress have more clout in terrorism investigations stemming from their constitutional war powers, as reflected in the preamble and operative provisions of the 2001 Authorization for Use of Military Force.[182] Thus, unlike traditional transnational criminal investigations involving narcotics trafficking for example, the foreign affairs and national security implications of terrorism investigations trigger constitutional and statutory support for U.S. involvement. Perhaps the constitutional might of the President's Commander-in-Chief and

177. *Id.*

178. *Id.*

179. *Id.* at 302.

180. *Id.* at 305–06.

181. United States v. Maturo, 982 F.2d 57, 61 (2d Cir. 1992); United States v. Delaema, 583 F. Supp. 2d 104, 107 (D.D.C. 2008).

182. Authorization for the Use of Military Force, Pub. L. No. 107-40, 115 Stat. 224 (2001).

defensive war powers[183] puts the "evading the Constitution" requirement in a new context. The additional constitutional support may reinforce or even mandate U.S. law enforcement's involvement with search and seizures connected to terrorist threats abroad. The national security implications of terrorism may place these searches on higher constitutional footing than similar criminal investigations abroad, overriding evasion concerns. Since collaborative counterterrorism investigations implicate national security and foreign relations, areas where more authority and discretion is traditionally lodged within the Executive,[184] the "evading the constitution" component of joint venture analysis may lose its significance and weight in this context. Critics may stress, however, that courts must strictly interpret this standard to preserve the constitutional limits on terrorism investigations, where the executive is prone to sacrifice privacy for security.

3. Technology Camouflages Conventional Joint Ventures

While the twenty-first century expands the range of activities that could be considered joint ventures, the addition of technology to searches and seizures may transform joint ventures into mere participation, leading courts to admit evidence in situations where they previously would have excluded it. For instance, under the current joint venture test, a U.S. agent abroad who spots a suspected terrorist and informs local authorities seems to fall closer to a joint venture than a U.S. satellite that spots the same terrorist and passes identical information to local authorities. As alluded to in the discussion of the substantiality component of the joint venture exception, removing the human element may eradicate some of the concern about constitutional evasion, manipulation or abuse by police. Nevertheless, when police can use technology to achieve the same ends—for instance, conducting a remote search of a U.S. person's computer located abroad rather than sending U.S. agents to raid an apartment—the means should not alter the action's constitutionality. Unfortunately, the joint venture case law, which distinguishes between "mere presence" of the U.S. government in the search (which did not suffice to

183. United States v. Curtiss-Wright Export Corp., 299 U.S. 304, 319–22 (1936); The Prize Cases, 67 U.S. 635, 670 (1863).

184. *Curtiss-Wright*, 299 U.S. at 319–21; *The Prize Cases*, 67 U.S. at 670.

be a joint venture)[185] and the "actual coordination of investigation and control" (which was a joint venture),[186] does not easily adapt to the evolution in investigative methods.

Another example helps illustrate this problem. Rather than assist a foreign police search by physically sending an agent who can recognize the suspect, U.S. agents can remotely employ facial recognition software to correctly identify the subject of the search. While the prior situation may be considered a joint venture under the traditional standards, is the latter? While there is no physical agent on the ground, the remote identification achieves the same purpose. Does the technology provide the necessary distance to push the interaction from actual involvement to the constitutionally unprotected zone of mere participation? If so, then technological advances may allow federal authorities to participate in unreasonable foreign searches in ways that were previously disallowed. Furthermore, technology like remote cross-border searches, in which law enforcement officials use computers within their own country to access files or data physically stored in another country,[187] may seem less invasive than traditional physical searches. Researchers at Purdue University are developing a system that uses cell phones to detect and track radiation to prevent detonation of dirty bombs or nuclear weapons.[188] Each cell phone would be equipped with radiation sensors, and if one detected even trace amounts of radiation a signal would be sent to local authorities.[189] Many also propose using high-tech surveillance to ensure security of cargo shipments, by attaching sensors with imaging capability, like RFID (radio-frequency identification) tags, to each container to track its position and to view its contents.[190] As these examples illustrate, the changing nature of technology itself may allow authorities to erect a legal barrier between their involvement and the search itself in order to dodge exclusion of any evidence gathered by foreign officials as a result of the search.

185. United States v. Behety, 32 F.3d 503, 511 (11th Cir. 1994) (finding that DEA agent present during a search of U.S. vessel by Guatemala officials not enough of a joint venture for exclusion).

186. Lustig v. United States, 338 U.S. 74, 78–79 (1949) (holding that presence of U.S. officers at investigation was enough to find joint venture).

187. *See* Patricia L. Bellia, *Chasing Bits Across Borders*, 2001 U. CHI. LEGAL F. 35, 39–40 (2001).

188. *Thwarting Nuclear Terrorism Using Cell Phone Sensors*, MED. NEWS TODAY, Jan. 23, 2008, http://www.medicalnewstoday.com/articles/94761.php.

189. *Id.*

190. Lin et al., *supra* note 6, at 158–59.

C. *Normative and Policy Concerns*

Even if technology does weaken the joint venture exception to the silver platter doctrine, is this necessarily worrisome? While some may argue that the diluted joint venture test fails to adequately protect longstanding fourth amendment values, the transnational terrorist threat and the globalized nature of society may require this change. Part 1 evaluates whether the expanded scope of the international silver platter doctrine is normatively a positive development in the context of terrorism investigations. Part 2 suggests that the exclusionary rule may not be a suitable remedy for questionable products of joint foreign searches and explores alternative solutions. Finally, Part 3 considers which branch of government should decide how to strike the balance between national security interests and fourth amendment protections in collaborative counterterrorism searches against U.S. persons abroad.

1. Looser Admissibility Standards: A Normative Good or Evil?

Counterterrorism investigations sit at the legally uncertain intersection of intelligence and law enforcement, thus making it difficult to determine which legal standards investigators must follow.[191] On both ends of the spectrum, scholars can categorize terrorism as either (1) a foreign affairs threat to national security governed by the laws of war and conducted by the political branches or (2) a traditional crime which must be investigated in accordance with fourth amendment standards and monitored by the courts.[192] Since terrorism likely falls somewhere between these two extremes, which legal framework should govern?[193] Notably, the Obama administration's decision to prosecute 9/11 defendants in civilian courts[194] and to subject Umar Farouk Abdulmutallab to civilian rather than military ju-

191. Ronald J. Sievert, *War on Terrorism or Global Law Enforcement Operation?*, 78 NOTRE DAME L. REV. 307 (2003).

192. *Id.* at 308.

193. *Id.* at 335 ("[O]ur armed forces and intelligence agents could potentially face difficult legal obstacles in attempting to conduct foreign searches against terrorist suspects who are American citizens where our clear intent is criminal prosecution.").

194. Peter Finn & Carrie Johnson, *Alleged Sept. 11 Planner Will Be Tried in New York*, WASH. POST, Nov. 14, 2009, http://www.washingtonpost.com/wp-dyn/content/article/2009/11/13/AR2009111300740.html (reporting that the "self-proclaimed mastermind of the Sept. 11, 2001 attacks, and four co-conspirators will be tried in Manhattan federal courthouse").

risdiction,[195] suggests that in some circumstances criminal law applies to terrorism investigations.[196]

By expanding the international silver platter doctrine and narrowing its joint venture exception, the standards highlighted above provide for more flexible admission of evidence gathered in foreign searches abroad. From a policy perspective, these changes may actually support counterterrorism efforts at both the investigative stage and the prosecutorial stage. By loosening the rigid fourth amendment evidentiary standards in this context, investigators have the flexibility necessary to foster cooperation among foreign states, to employ new methods to combat an expansive underground terrorism threat and to expand their focus globally to events around the world that could cause instant disaster for the United States. Thus, the accidental impact of technology and globalization on the application of the international silver platter doctrine has coincidentally made that doctrine more amenable to the twenty-first century terrorist threat.

But from the defendant's perspective, the loosened standards give the prosecutor a distinct advantage and raise concerns of abuse and constitutional violations.[197] More significantly, the transformation in the international silver platter doctrine may not be contained to the terrorism context. Technology and globalization have fostered other types of global threats that lack the national security and foreign policy implications of terrorism. For instance, transnational drug trafficking, cybercrime, global white collar fraud and global racketeering schemes have analogous transnational characteristics that may also garner the special expanded international silver platter treatment. When these "traditional" crimes are disguised by technology and globalization, evidence that should be excluded under

195. Letter from Eric Holder, U.S. Att'y Gen., to Mitch McConnell, U.S. Sen. (Feb. 3, 2010) (available at http://www.justice.gov/cjs/docs/ag-letter-2-3-10.pdf) (outlining the Attorney General's rationale for charging Umar Farouk Abdulmutallab in federal court).

196. This decision has invited enormous debate and criticism over whether to try national security cases in criminal courts, military tribunals or special national security courts. *See, e.g.*, Jane Mayer, *The Trial: Eric Holder and the Battle over Khalid Sheikh Mohammed*, NEW YORKER, Feb. 15, 2010, http://www.newyorker.com/reporting/2010/02/15/100215fa_fact_mayer (highlighting the debate regarding whether the 9/11 defendants should be tried in civilian court and noting the Obama Administration's reconsideration of its original decision).

197. Motz's dissent in *Abu Ali* argues that the majority's refusal to find a joint venture "permits United States law enforcement officers to strip United States citizens abroad of their constitutional rights simply by having foreign law enforcement officers ask the questions. This cannot be the law." United States v. Abu Ali, 528 F.3d 210, 231 n.6 (4th Cir. 2008).

strict fourth amendment standards may be admissible. Thus, with reduced evidentiary standards in collaborative searches bleeding into traditionally criminal cases, we may sacrifice fourth amendment rights in the long run, especially as crime becomes more global and technological in nature and as the United States has to reach out to foreign partners to help investigate it.[198] If the expansion of the international silver platter doctrine is not strictly limited to cases where national security and foreign policy are implicated, it may eventually undermine the Fourth Amendment and Constitution as a whole.[199]

2. Appropriate Remedy: Alternatives to the Exclusionary Rule

In light of these policy debates, perhaps exclusion of evidence is not the best approach for protecting fourth amendment values in counterterrorism searches. The original purpose of excluding evidence from trial is to deter U.S. officials from conducting unreasonable searches and seizures. The exclusionary rule, however, seems ill-equipped to remedy unreasonable searches and seizures in the counterterrorism context because (1) exclusion may not deter unreasonable searches and (2) even if it does deter, that deterrence may come at a high cost to counterterrorism efforts worldwide. The stakes are much higher in terrorist investigations than in typical criminal investigations. As the September 11th attacks make painfully clear, a successful attack can wreak global devastation—claiming thousands of lives and undermining the world economy for years to come. Thus, unlike most criminal investigations, terrorism investigations are preemptive rather than reactive, focusing primarily on containing and neutralizing threats as quickly and as efficiently as possible. Gathering evidence for future criminal prosecutions is a far less important secondary concern, making it unlikely that the exclusionary rule will achieve its deterrence objective in terrorism investigations.

198. *See* LAURA K. DONOHUE, THE COST OF COUNTERTERRORISM: POWER, POLITICS, AND LIBERTY (2008) (exploring how loopholes in British procedure, which were created to deal with difficult cases, ended up changing the procedural rules in all cases).

199. Michael B. Mukasey, *Jose Padilla Makes Bad Law*, WALL ST. J., Aug. 22, 2007, *availabe at* http://www.americanbar.org/content/dam/aba/migrated/2011_build/law_national_security/mukasey_padilla_wsj.authcheckdam.pdf (considering "distortions that arise from applying to national security cases generally the rules that apply to ordinary criminal cases" and commenting that "if conventional legal rules are adapted to deal with a terrorist threat, whether by relaxed standards for conviction, searches, the admissibility of evidence or otherwise, those adaptations will infect and change the standards in ordinary cases with ordinary defendants in ordinary courts of law.").

Second, in the counterterrorism context the deterrence objective faces countervailing policy considerations. Even though the deterrence motivation behind applying the Fourth Amendment to extraterritorial searches is strained, some argue that exclusion of evidence gathered illegally by foreign police with U.S. collaboration may discourage U.S. involvement in cooperative international searches altogether. As an illustration, suppose courts interpret joint venture broadly, excluding the products of virtually all foreign searches involving U.S. authorities. If the United States provides technological assistance to foreign police in a terror investigation—like forwarding data from sensors, satellite imagery or advanced surveillance systems—and the foreign state conducts an unreasonable search (one violating foreign law), the evidence will be excluded from a subsequent U.S. criminal trial. The interconnected nature of the threat, however, makes joint ventures so common that the effect of the exclusion may be to deter the United States from collaborating (openly at least) with law enforcement forces known to bend their rules.[200] Since these are often the countries most plagued by terrorist activity and least technologically savvy, rather than deterring unreasonable searches, a broad joint venture test may undermine coordination between law enforcement in the regions where it is most needed—allowing terrorists to use these nations as safe-havens, undermining global counterterrorism efforts and exposing the United States and its allies to potentially deadly attacks.

To determine whether the burden of the joint venture exclusion is too great to apply in the terrorism context we must ask whether imposing the exclusionary rule on evidence gathered in these joint efforts would undermine international partnerships. Notably, remote coordination facilitated by technology is far more common than conventional physical assistance. So if the exclusionary rule did have a negative impact on collaboration, the extent of the damage on inter-

200. Vladeck, *supra* note 164, at 1518 n.126, similarly argues, in the Fifth Amendment context, that finding a joint venture and excluding un-Mirandized statements to Saudi authorities would reap dangerous public policy consequences:

> [S]uch a broad per se holding [requiring Miranda protection] could potentially discourage the United States and its allies from cooperating in criminal investigations of an international scope. . . . To impose all of the particulars of American criminal process upon foreign law enforcement agents goes too far in the direction of dictation, with all its attendant resentments and hostilities. Such an unwarranted hindrance to international cooperation would be especially troublesome in the global fight against terrorism, of which the present case is clearly a part.

(citing *Abu Ali*, 528 F.3d at 230 n.5).

national law enforcement working relationships would be far-reaching.

If the exclusionary rule is not the appropriate tool to guard fourth amendment values in the terrorism investigations, what other mechanisms effectively protect U.S. citizens from unreasonable cooperative foreign searches and seizures? First, judges could impose less drastic remedies to correct for questionable evidence that escapes fourth amendment requirements via the international silver platter doctrine. For example, through procedural mechanisms, the court could provide a limiting jury instruction, impose an inference on the evidence or limit cross examination in order to correct for any improper influence. The court could also admit the fruits of an unreasonable joint venture, but later allow the subject of the search to bring a civil suit for a constitutional violation against federal officers seeking nominal damages.[201] Second, the political process may check the activities of law enforcement. Since counterterrorism investigations are shrouded in secrecy, however, the lack of transparency will likely prevent the public from recognizing abuses and voting on that basis. Further, since the wounds from September 11th are still fresh, the public is not likely to vote in favor of extending more search protections to terrorism suspects. Third, international and foreign law may also provide some level of protection. Since foreign law enforcement relationships are critical to combating terrorism, international legal rules regarding searches and seizures may have some impact. Further, under fourth amendment doctrine, a foreign search is only unreasonable if the foreign officials do not comport with their own law, because foreign law defines the suspect's reasonable expectation of privacy. Thus, when searches are conducted abroad, the contours of foreign law determine individuals' fourth amendment protections.

Up until this point, this Note, with its exclusive focus on evidentiary rules and exclusion, has implied that the courts are the sole branch responsible for regulating the conduct of our law enforcement abroad. This assumption, however, is fundamentally flawed. As explained below, the executive and legislative branches may have more important roles in regulating counterterrorism searches and seizures. Notably, potential remedies for violations hinge on the branch of government responsible for defining, regulating and overseeing U.S. involvement in foreign searches. The following Section, while at-

201. Christopher D. Totten, *New Federalism and Our Constitutional Rights in the Criminal Context*, 46 CRIM. L. BULL. 515, 526 (2010).

tempting to answer this institutional balancing question, presents alternatives to court-enforced remedies.

3. Institutional Questions

Finally, we must address which branches of government are best equipped to decide the issues surrounding the application of the exclusionary rule to evidence gathered abroad in joint counterterrorism investigations. Institutionally, each government actor plays a different role suited to its constitutional allocation of national security powers and its own institutional capabilities. Each of the branches are endowed with different levels of authority to (1) set the policy for, or tactically coordinate with, foreign authorities to conduct searches abroad, (2) regulate the conduct and define the obligations of U.S. law enforcement in foreign searches and (3) police whether law enforcement complies with the Fourth Amendment and impose remedies for violations. The push and pull between the branches over these roles further complicates the fourth amendment international silver platter doctrine analysis, revealing how collaborative counterterrorism investigations pose a unique evidentiary problem and suggesting that traditional criminal courts may not be the best institution for making these types of evidentiary decisions.

Many scholars and the Supreme Court propose various ways to strike a balance among the executive, Congress and the courts in national security decision making.[202] Most obviously, courts seem to play an important role in policing the executive and law enforcement in national security cases, especially when the executive makes a policy decision to charge a terrorism suspect in criminal court.[203] Even in this context, however, some may question both the competence and the influential effect of a judiciary ruling on law enforcement tactics abroad.[204] First, even though the courts have developed the

202. Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 634 (1952) (Jackson, J., concurring). For scholarly commentary, see *infra* notes 204, 206, 209 and accompanying text.

203. THE FEDERALIST NO. 78 (Alexander Hamilton) (noting that the judiciary needs to be independent to check the political branches and to shield liberty). Some argue that the judiciary should be active in balancing national security issues, especially during national security crises and war, and highlight the importance of a vigilant judiciary that can counter executive attempts to curtail civil liberties. Doe v. Ashcroft I, 334 F. Supp. 2d 471, 478 (S.D.N.Y. 2004), *vacated*, Doe v. Gonzales, 449 F.3d 415 (2d Cir. 2006).

204. Many scholars suggest that courts should be involved in decisions on the Fourth Amendment and technology. "When technology threatens privacy, the thinking goes, the courts and the Constitution should offer the primary response. While Congress and state

existing international silver platter doctrine, the judicial branch may not have the capabilities and resources to effectively lay out comprehensive guidelines in counterterrorism investigations.[205] Institutionally, courts may not have the willpower, expertise or legitimacy to make a determination on such highly sensitive issues as terrorism, international partnerships and law enforcement needs. During wartime many argue that courts lack judicial expertise to review intelligence and tactical war decisions,[206] stressing that courts should defer to executive judgment on the appropriate methods for coordinating searches and investigations abroad to prevent terrorism strikes.[207] Since the judiciary has a long history of deferring to presidential tactical decision making during war,[208] perhaps this deference has been incorporated into the evidentiary standards governing international terrorism investigations through a broad interpretation of the international silver platter doctrine with a narrow joint venture exception.[209]

---

legislatures may have a limited role regulating government investigations involving new technologies, the real work must be done by judicial interpretations of the Fourth Amendment." Kerr, *supra* note 132, at 802–04. Kerr, however, argues against a strong judicial role in defining the Fourth Amendment with respect to changes in technology:

> [C]onsiderations of doctrine, history, and function tend to counsel against an aggressive judicial role in the application of the Fourth Amendment to developing technologies . . . . [C]ourts should place a thumb on the scale in favor of judicial caution when technology is in flux, and should consider allowing legislatures to provide the primary rules governing law enforcement investigations involving new technologies.

Kerr, *supra* note 132. at 805.

205. While the circuits have all spelled out different joint venture standards, the Supreme Court has yet to tackle the issue.

206. Alberto Gonzales, *Waging War with the Constitution*, 42 TEX. TECH. L. REV. 843, 883–84 (2010).

207. *Id.* ("[T]he complicated and insidious nature of this conflict with a non-state actor also argues for the courts to give even greater deference to the President and to the Congress as they develop the most effective strategies to protect America.").

208. *Id.* For more decisions urging deference to the executive, see *Ludecke v. Watkins*, 335 U.S. 160 (1948) and *The Prize Cases*, 67 U.S. 635, 670 (1863) ("[W]hether the President in fulfilling his duties, as Commander-in-Chief, in suppressing an insurrection, has met with such armed hostile resistance, and a civil war of such alarming proportions as will compel him to accord to them the character of belligerents, is a question to be decided *by him*, and this Court must be governed by the decision and acts of the political department of the Government to which this power was entrusted." (emphasis in original)).

209. In the analogous fifth amendment joint venture context, one scholar stresses "the difficulties courts face in applying precedents forged in traditional law enforcement to multinational counterterrorism investigations." Vladeck, *supra* note 164, at 1503 (explaining the evidentiary difficulties in *United States v. Abu Ali*, 528 F.3d 210 (4th Cir.

Second, since terrorism prosecutions are infrequent,[210] courts rarely have the opportunity to evaluate the definition of "joint venture" in the international silver platter doctrine and to articulate uniform fourth amendment requirements for cooperative counterterrorism searches, which significantly hinders the courts' ability to substantively influence the conduct of officers abroad. Further, since agents primarily work to prevent catastrophic attacks rather than preserve a future prosecution, judges may realize that any substantive evidentiary rules elaborated may have little effect on the conduct of officers in the field. These considerations make courts more likely to admit evidence based on the silver platter doctrine, without broadly applying the Fourth Amendment to products of all cooperative foreign searches.

Others argue that the executive should determine how to best balance the needs for transnational cooperation with our fourth amendment constitutional requirements.[211] As the director of our foreign affairs,[212] leader of our intelligence community and law enforcement forces and our Commander-in-Chief, the President is arguably in the best position to make decisions about terrorism investigations. The executive has the speed, expertise and resources to lay out counterterrorism strategies and respond quickly to ongoing threats.[213] Some argue that in order to avoid evidentiary problems, counterterrorism investigations should be made predominantly military in nature, in order to "facilitate intelligent decisions when the inevitable conflicts arise between the philosophy and culture of the mil-

---

2008)). Vladeck stresses the unique challenges judges face in terrorism cases, by attempting to fit novel fact patterns into an old procedural framework.

> The principled disagreement over whether Abu Ali's interrogation constituted a "joint venture" raises an important and contested question of constitutional criminal procedure that turns in no meaningful substantive way on the fact that his was a terrorism trial, as opposed to a trial for any other offense over which the federal courts have jurisdiction.

Vladeck, *supra* note 164, at 1531–32.

210. Mukasey also argues that criminal terrorism prosecutions have not yielded many convictions, though they have imposed high financial burdens on the federal courts. Mukasey, *supra* note 199.

211. *See* Sievert, *supra* note 82, at 351–53.

212. United States v. Curtiss-Wright Export Corp., 299 U.S. 304, 319 (1936).

213. THE FEDERALIST NO. 70 (Alexander Hamilton) ("Decision, activity, secrecy, and dispatch will generally characterize the proceedings of one man in a much more eminent degree than the proceedings of any greater number. . . . In the legislature promptitude of decision is oftener an evil than a benefit. . . . In the conduct of war, in which the energy of the executive is the bulwark of the national security, everything would be to be apprehended from its plurality.").

itary and law enforcement, and [to] prevent mixed messages that can potentially undermine the overall anti-terrorist effort."[214] While military-led investigations may bolster the war effort and stem the tide of terrorism, many worry that self-policing will not provide a check on the executive or a bulwark for civil liberties.

Rather than leave these tricky evidentiary decisions entirely to the courts or to the executive, perhaps Congress should establish the rules governing evidence gathered in counterterrorism investigations. Scholars propose that Congress "clarify procedures for extraterritorial search and seizure in criminal cases" in order to equip our law enforcement to combat the twenty-first century terrorist threat,[215] especially when it comes to changing technology.[216] Kerr argues that

> [t]he institutional advantages of legislative rule making may eventually create a bifurcated privacy regime in which the governing law is primarily constitutional in most areas, but primarily statutory in areas of technological flux. Technological change may reveal the institutional limits of the modern enterprise of constitutional criminal procedure, exposing the need for statutory guidance when technology is changing rapidly. . . . If criminal prosecutions involving new technologies continue to grow in number and importance, a basic understanding of criminal procedure rules may someday require as much knowledge of the United States Code as the United States Reports. [217]

Kerr's analysis with regard to changing technologies could apply equally to the globalization and technology considerations embodied within the terrorism threat.

---

214. Sievert, *War on Terrorism*, *supra* note 191, at 352 ("The military role need not be exclusive, but it must be made clear that it is predominant.").

215. Sievert, *supra* note 82, at 1464.

216. Kerr suggests that "the legislative branch rather than the judiciary should create the primary investigative rules when technology is changing," while noting that "legislative predominance in the face of developing technologies is consistent with current Fourth Amendment doctrine, accurately reflects historical practice, and is likely to continue in the future given the relative institutional competence of courts and legislatures." Kerr, *supra* note 132, at 806.

217. *Id.*

If courts are not institutionally competent to pronounce substantive evidentiary rules for terrorism investigations,[218] Congress should establish statutory rules. Crucially, while the executive sets national security and intelligence policy by making tactical decisions for specific searches, Congress also has a role in circumscribing operational policy by regulating and defining the duty of agents conducting foreign searches. Unless Congress steps in to establish definitive rules, technological developments and international collaboration will continue to reduce the practical application of the Fourth Amendment to collaborative searches abroad. Once Congress establishes the framework, then the courts can uniformly police whether the government complies with its fourth amendment obligations.

CONCLUSION

As security threats and technology continue to evolve, the fourth amendment doctrine should similarly develop to meet these changes.[219] The widened interpretation of international silver platter doctrine in the twenty-first century has brought about this very evolution in the Fourth Amendment—perhaps suggesting that criminal law standards articulated by courts can transform according to the demands of the unique investigatory context of counterterrorism without the input of the political branches. Nevertheless, while the rise of international terrorism and transnational law enforcement cooperation demands to some extent a broad international silver platter doctrine and a narrow joint venture exception, at some point Congress must legislate rules of conduct to preserve a baseline of fourth amendment values governing cooperative searches of Americans abroad. Without such protection, the loosening of the fourth amend-

218. *Id.* at 807–08 ("Courts also lack the information needed to understand how the specific technologies in cases before them fit into the broader spectrum of changing technologies, and cannot update rules quickly as technology shifts. Legislatures do not offer a panacea, but they do offer significant institutional advantages over courts. Legislatures can enact comprehensive rules based on expert input and can update them frequently as technology changes. As a result, legislatures can generate more nuanced, balanced, and accurate privacy rules when technology is in flux. Courts should recognize their institutional limitations and remain cautious until the relevant technology and its applications stabilize.").

219. *See* Kerr, *supra* note 132, at 804 (urging a broad fourth amendment interpretation in order to respond to technological changes); Sievert, *supra* note 82 (exploring the necessary flexibility given to law enforcement officials in the Constitution to combat terrorism threats, specifically addressing whether the law sufficiently protects the public and what changes must be made to successfully combat terrorism).

ment doctrine in cooperative counterterrorism searches is likely to extend to more conventional criminal investigations as crime becomes more global and technological in nature.

Caitlin T. Street[*]

* J.D. Candidate, Columbia Law School, 2011; B.A. College of the Holy Cross, 2008. I would like to thank Professor Matthew Waxman for his guidance, insight and generous feedback throughout the evolution of this Note. I would also like to express my gratitude to the staff of *The Columbia Journal of Transnational Law*, especially Katherine Kenney and Jacqueline Bonneau, for their diligent editorial assistance and patience. Finally, I would like to thank my parents for their unwavering support and invaluable encouragement, which have made all my pursuits, this Note included, possible.