Marquette Law Review

Volume 96
Issue 1 *Fall 2012*

Article 8

Quis Custodiet Ipsos Custodes? Limits on Widespread Surveillance and Intelligence Gathering By Local Law Enforcement After 9/11

Craig Roush

QUIS CUSTODIET IPSOS CUSTODES?[1] LIMITS ON WIDESPREAD SURVEILLANCE AND INTELLIGENCE GATHERING BY LOCAL LAW ENFORCEMENT AFTER 9/11

In the decade since the terrorist attacks of September 11, 2001, local law enforcement has become the front line in the nation's counterterrorism strategy. This involvement has not come without controversy. As part of these counterterrorism efforts, police departments have begun to establish widespread surveillance and intelligence-gathering networks to monitor Muslim and other ethnic neighborhoods in the hopes of stopping the next terrorist attack at its source. Such surveillance does not necessarily run afoul of the Constitution, and both our political environment—in which voters demand that the government stop terrorism at all costs—as well as unprecedented levels of federal funding to fight terrorism have made these surveillance programs an attractive option for local law enforcement. But the same programs risk compromising citizens' civil liberties and damaging police relationships with ethnic communities. This Comment analyzes whether and how a balance might be struck between national security and individual civil liberties interests, and offers a model statutory solution drawn from police surveillance in a non-terrorism-related context as one possible way forward.

1. Literally translated from the Latin, "Who will guard the guards themselves?," *see* GABRIEL G. ADELEYE & KOFI ACQUAH-DADZIE, WORLD DICTIONARY OF FOREIGN EXPRESSIONS: A RESOURCE FOR READERS AND WRITERS 332 (Thomas J. Sienkewicz & James T. McDonough eds., 1999), though the phrase is sometimes translated more figuratively as "Who watches the watchmen?" One of the most famous epigrams, it appears in Juvenal's *Satire VI*. JUVENAL: THE SATIRES 200 (John Ferguson ed., 1979). Juvenal was a Roman satirist of the first and second centuries; although little is known about his life, including the dates of his birth, death, and authorship of the satires, most estimates place the satires between 110 and 120 A.D. CHRISTOPHER KELK, THE SATIRES OF JUVENAL: A VERSE TRANSLATION ix (2010).

I. INTRODUCTION

Late in his majority opinion in the 1983 Supreme Court case of *United States v. Knotts*, in which police placed a criminal suspect under continuous surveillance[2] to discover the location of his secret lair, then-Associate Justice William Rehnquist addressed the defendant's argument that allowing police to conduct such surveillance without a warrant was a slippery slope that would ultimately lead to "twenty-four hour surveillance of any citizen of this country . . . without judicial knowledge or supervision."[3] As members of the Court are wont to do when dealing with hypothetical fact patterns, Justice Rehnquist punted, writing that "if such dragnet-type law enforcement practices as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable."[4] In hindsight, Justice Rehnquist's response can hardly be called regrettable; at the time, long-term surveillance was typically subject to multiple levels of review and only implemented if the benefits outweighed the costs.[5] And so it was that the Court upheld the use of the tracking device, Knotts lost his appeal, and Justice Rehnquist's promise was consigned to the dusty pages of volume 460 of the *United States Reports*.

Perhaps, that is, until now. At the beginning of the twenty-first century, a series of unexpected events has made systematic, widespread, twenty-four-hour surveillance of not just individuals but entire neighborhoods and cities a reality.[6] This series of events began with the terrorist attacks of September 11, 2001, which prompted a seismic shift

---

2. United States v. Knotts, 460 U.S. 276, 276-80 (1983). *Knotts*, which involved the use of a primitive GPS tracking device, is discussed in more detail *infra* in Part III.C.1; *see also infra* note 145 (discussing the Supreme Court's recent decision in another case involving GPS tracking devices, United States v. Jones, 132 S. Ct. 945 (2012), and its potential impact on Fourth Amendment jurisprudence). But note that the defendant's argument—and the scope of this Comment—both focus on broader surveillance practices, of which GPS tracking devices are only a subset.

3. *Knotts*, 460 U.S. at 283 (quoting Brief for Respondent at 9, *Knotts*, 460 U.S. 276 (no. 81-1802)).

4. *Id.*

5. For example, in the 1980s, the FBI's Undercover Operations Review Committee reviewed undercover operations and classified them as either Group I or Group II investigations; those classified as Group I—because they were expected to cost more than $20,000, last longer than six months, or involve "sensitive circumstances"—were subject to multiple layers of approval and a multi-factor cost–benefit analysis. GARY T. MARX, UNDERCOVER: POLICE SURVEILLANCE IN AMERICA 183 (1988).

6. *See infra* Part II.B for some of the most high-profile examples from recent years.

in our nation's security priorities that has penetrated to the lowest levels of local government. As part of this shift, the federal government has poured unprecedented levels of funding into local police departments, removing many of the economic barriers to extended, widespread police surveillance and intelligence gathering that previously existed.[7] As a result, police surveillance is now testing the boundaries of constitutional jurisprudence in ways that—as Justice Rehnquist may have assumed in 1983—would never have seemed likely, or even possible.

This Comment undertakes the analysis that might occur if, thirty years later, we were to field Justice Rehnquist's punt in *Knotts* and assess whether constitutional principles may be applicable to such surveillance—and if not, what the next-best solution for protecting individuals' civil liberties might be. It begins in Part II with an overview of the events during the last decade that have led us to this point, describing the shift in national priorities that followed September 11, 2001, and detailing two of the more infamous cases of widespread police surveillance and intelligence gathering that have surfaced in recent years.[8] Part III assesses whether constitutional principles are applicable to this new surveillance, namely, the Fourth Amendment's protections of individuals' privacy through its prohibition on unreasonable searches and seizures. In an effort to illuminate the present state of Fourth Amendment jurisprudence, Part III also dives into the Amendment's historical roots and discusses three key exceptions to its general rule. Finding the Fourth Amendment's protections inadequate, Part IV discusses the next-best alternative, statutory protections, and the competing interests—national security and individuals' privacy—that must be taken into account when drafting potential legislation. Finally, Part V returns to the present, drawing upon a recent instance of police surveillance and intelligence gathering conducted on anti-death penalty activists in Maryland to develop a model statutory solution that strikes a balance between protecting citizens' civil liberties and affording police the latitude to conduct investigation when the need arises. Part V goes

7. *See infra* Part II.A.

8. Because this Comment is primarily concerned with widespread police surveillance and intelligence gathering conducted by local law enforcement agencies, it does not discuss past federal programs such as the U.S. Defense Department's Counterintelligence Field Activity database or the TALON reporting mechanism. For a discussion of these topics, see Lisa Myers et al., *Is the Pentagon Spying on Americans?*, NBCNEWS.COM (Dec. 14, 2005, 6:18 PM), http://www.msnbc.msn.com/id/10454316/ns/nbcnightlynews-nbc_news_investigates/t/pentagon-spying-americans/.

on to analyze how such a model statute might have helped to mitigate some of the police conduct detailed in Part II. Part VI concludes.

II. COUNTERTERRORISM AND LOCAL LAW ENFORCEMENT AFTER SEPTEMBER 11, 2001

In the decade following the September 11, 2001 terrorist attacks in New York City, Washington, D.C., and Pennsylvania, the United States understandably redirected a significant portion of its national resources toward counterterrorism and homeland security.[9] But while a shift in *national* priorities was inevitable—given that homeland security has a primarily national scope—an equivalent shift in state and local law enforcement priorities may not have been as predictable. As this Part will show, however, that shift has occurred. Local law enforcement agencies are now widely involved in counterterrorism activities in a variety of capacities, including (and in some cases, especially) surveillance and intelligence gathering. With this increased involvement, however, has come an unfortunate side effect: counterterrorism surveillance and intelligence-gathering operations implemented by local law enforcement agencies have brushed against constitutional protections of individuals' privacy and civil liberties. This Part will first provide a summary of the changes that have occurred with respect to local law enforcement and counterterrorism priorities over the last decade, and then review some of the more recent examples of police activity that have aroused concerns over civil liberties.

A. The Transformation of Local Law Enforcement Following September 11, 2001

As some have noted, "the most striking feature" of law enforcement in the United States is its decentralization.[10] There are about 600,000 to

9. The Department of Homeland Security (DHS) was established on Nov. 25, 2002, by the Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (codified as amended in scattered sections of 6 U.S.C.). The Act brought twenty-two different federal agencies under DHS's authority. Donald F. Kettl, *Overview*, *in* THE DEPARTMENT OF HOME LAND SECURITY'S FIRST YEAR: A REPORT CARD 1, 1 (Donald F. Kettl ed., 2004). In the year following the creation of DHS, the number of federal government employees focused on homeland security doubled; today, DHS has 183,000 employees, making it the third-largest Cabinet-level department, after the Department of Defense and the Department of Veterans Affairs. U.S. Office of Pers. Mgmt., *Executive Branch Civilian Employment Since 1940*, FED. EMP. STAT. (Sept. 30), http://www.opm.gov/feddata/HistoricalTables/ExecutiveBranchSince1940.asp.

10. David Thacher, *The Local Role in Homeland Security*, 39 LAW & SOC'Y REV. 635,

700,000 local police officers in the United States,[11] spread out among somewhere from 13,000 to 19,000 local law enforcement agencies across the country.[12] Despite the fact that local law enforcement accounts for the majority of crime fighting in the United States,[13] its experience with counterterrorism and national security prior to September 11, 2001, was minimal.

Instead, over the years, local law enforcement has been drawn into the national security arena only occasionally—for example, after World War I,[14] both before and after World War II,[15] and again during the 1980s[16] and early 1990s[17]—and never for any consistent purpose. The result was that, by the mid-1990s, many states had enacted statutes criminalizing terrorist activities,[18] yet less than half of all local law enforcement agencies had developed contingency plans for terrorist

635 (2005).

11. *See id.* (estimating more than 600,000 local law enforcement officers in the United States); David E. Kaplan, *Spies Among Us*, U.S. NEWS & WORLD REP., May 8, 2006, at 40, 43 (estimating over 700,000 officers).

12. *See* Thacher, *supra* note 10, at 635 (counting nearly 13,000 local law enforcement agencies in the United States); Matthew C. Waxman, *Police and National Security: American Local Law Enforcement and Counterterrorism After 9/11*, 3 J. NAT'L SECURITY L. & POL'Y 377, 380 (2009) (finding sources that cite up to 19,000 agencies).

13. Waxman, *supra* note 12, at 380.

14. In 1919 and 1920, local police assisted the Bureau of Investigation (the predecessor to the modern-day Federal Bureau of Investigation, or FBI) in the Palmer Raids, a series of mass arrests of suspected left-wing radicals. *Id.* at 379.

15. In 1939, with World War II looming, President Franklin Roosevelt urged "all police officers, sheriffs, and all other law enforcement officers in the United States" to turn over any evidence regarding acts of "espionage, counterespionage, sabotage, subversive activities and violations of the neutrality law" to the FBI. Samuel J. Rascoff, *The Law of Homegrown (Counter) Terrorism*, 88 TEX. L. REV. 1715, 1715 (2010) (quoting 1 NAT'L COUNTERINTELLIGENCE CTR., A COUNTERINTELLIGENCE READER: AMERICAN REVOLUTION TO WORLD WAR II 177 (Frank J. Rafalko ed., 2004)). In the 1950s and 1960s, the FBI enlisted local law enforcement in its Counter-Intelligence Program, which was designed to gather information about "allegedly subversive political groups." Waxman, *supra* note 12, at 379.

16. In 1980, the FBI's New York City field office established the first Joint Terrorism Task Force in response to a series of domestic terrorism incidents. NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT: FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES 81 (2004) [hereinafter THE 9/11 COMMISSION REPORT].

17. The FBI's New York City Joint Terrorism Task Force allowed local law enforcement in New York City, as well as other federal agencies, to share information with the FBI and to become involved in the FBI's investigations—both throughout the 1980s and again after the first World Trade Center bombing in 1993. *Id.*

18. Waxman, *supra* note 12, at 381.

attacks,[19] and only about 60% of cities had been in contact with the federal government regarding terrorism-related issues.[20] Simply put, prior to September 11, 2001, "with the exception of one portion of the FBI, very little of the sprawling U.S. law enforcement community was engaged in countering terrorism."[21]

After the terrorist attacks of September 11, 2001, this began to change. On November 13, 2001, Attorney General John Ashcroft ordered all United States Attorneys to work with local law enforcement on counterterrorism measures.[22] In 2006, President George W. Bush reiterated the importance of local law enforcement to national security.[23] Across the political spectrum, there was no shortage of agreement in Washington that local law enforcement represented the country's "front line of defense against terrorism"[24] because, as one report put it, "[a]ll terrorism is local."[25]

For its part, Congress provided the financial backing to bring local law enforcement into the war on terror. The Homeland Security Act of 2002,[26] which established the Department of Homeland Security, also established an Office for State and Local Government Coordination;[27] one of the primary responsibilities of this office is to "assess, and

19. *Id.*

20. *Id.*

21. THE 9/11 COMMISSION REPORT, *supra* note 16, at 82.

22. Ashcroft issued a memorandum to all United States Attorneys in which he wrote that successfully countering the emerging threat of terrorism meant "law enforcement officials at all levels of government—federal, state, and local—must work together, sharing information and resources needed to both arrest and prosecute the individuals responsible and to detect and destroy terrorist cells before they can strike again." Memorandum from John Ashcroft, U.S. Attorney Gen., U.S. Dep't of Justice, to all U.S. Attorneys (Nov. 13, 2001), *available at* http://www.hsdl.org/?view&did=452215. Ashcroft's directive gave the nation's ninety-three United States Attorney offices less than three weeks to establish a protocol for terrorism-related information sharing with state and local law enforcement officials, and required that the protocol provide for the possibility of communication "24 hours a day, 7 days a week." *Id.*

23. *See* President George W. Bush, The White House, Address to the Nation on Immigration Reform (May 15, 2006) (transcript available at http://georgewbush-whitehouse.archives.gov/news/releases/2006/05/20060515-8.html).

24. Kaplan, *supra* note 11, at 42.

25. INT'L ASS'N OF CHIEFS OF POLICE, FROM HOMETOWN SECURITY TO HOMELAND SECURITY: IACP'S PRINCIPLES FOR A LOCALLY DESIGNED AND NATIONALLY COORDINATED HOMELAND SECURITY STRATEGY 3 (2005).

26. Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (codified as amended in scattered sections of 6 U.S.C.).

27. 6 U.S.C. § 361(a) (2006).

advocate for, the resources needed by State and local government to implement the national strategy for combating terrorism."[28] Since the Act's passage, the Department of Homeland Security has allocated more than $35 billion in federal funding to state and local governments to "strengthen[] [the] nation's ability to prevent, protect, respond to, recover from, and mitigate terrorist attacks, major disasters and other emergencies."[29] The largest two components of annual appropriation—together representing more than half of the entire block of annual funding—are the State Homeland Security Program and the Urban Areas Security Initiative, both of which are primarily aimed at funding local law enforcement agencies.[30]

Furthermore, since the passage of the Implementing Recommendations of the 9/11 Commission Act of 2007,[31] states must ensure that at least 25% of funding received through either the State Homeland Security Program or the Urban Areas Security Initiative is used for "law enforcement terrorism prevention activities."[32]

State and local law enforcement agencies have readily taken advantage of this funding, directing federal counterterrorism dollars into at least four different categories of terrorism-related activities at the local level, many of which would have been unheard-of—or at least

28. *Id.* § 361(b)(2).

29. *See* Press Release, U.S. Dep't. of Homeland Sec., DHS Announces More Than $2.1 Billion in Preparedness Grants (Aug. 23, 2011), *available at* http://www.dhs.gov/news/2011/08/23/dhs-announces-more-21-billion-preparedness-grants (describing the allocation of "approximately $35 billion" in grants for the period 2002–2011); Press Release, U.S. Dep't of Homeland Sec., DHS Announces More Than $1.3 Billion in Fiscal Year (FY) 2012 Preparedness Grant Awards (June 29, 2012), *available at* http://www.dhs.gov/news/2012/06/29/dhs-announces-more-13-billion-fiscal-year-fy-2012-preparedness-grant-awards [hereinafter FY 2012 DHS Grants].

30. For example, in the fiscal year 2012 appropriation (announced in June 2012) State Homeland Security Program (SHSP) grants totaled $294 million and Urban Areas Security Imitative (UASI) grants totaled $490 million. FY 2012 DHS Grants, *supra* note 29. Put together, this equals $784 million, or 60%, of the $1.3 billion in total preparedness grants issued by DHS that year. *See id*. The State Homeland Security Program (SHSP) funding "supports the implementation of state Homeland Security Strategies." *FY 2012 Homeland Security Grant Program*, FED. EMERGENCY MGMT. AGENCY (last updated July 12, 2012, 2:27 PM), http://www.fema.gov/fy-2012-homeland-security-grant-program. The Urban Area Security Initiative (UASI) provides funding to "address the unique . . . needs of high-threat, high-density urban areas, and assists them in building an enhanced and sustainable capacity to prevent, protect against, mitigate, respond to, and recover from acts of terrorism." *Id.*

31. Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, 121 Stat. 266 (codified in scattered sections of 6 U.S.C.).

32. 6 U.S.C. § 607(a)(1).

impractical—in a pre-September 11 world.[33] First, many local law enforcement agencies reassigned personnel to newly created or expanded counterterrorism departments.[34] Second, law enforcement began upgrading its technology and weaponry; recent counterterrorism acquisitions by local police include surveillance cameras,[35] SUVs that can detect nuclear radiation,[36] military-grade assault rifles,[37] and even an unmanned aerial vehicle.[38] Third, local law enforcement agencies have

33. *See supra* notes 26–32 and accompanying text (noting that the Homeland Security Act, which provided state and local law enforcement agencies with a substantial amount of federal funding, was passed in 2002, post-9/11).

34. *See, e.g.*, Chuck Bennett, *Shepherding Safe Subways*, NEWSDAY (New York), Nov. 28, 2006, at A6 (describing how the New York Police Department has deployed canine units "devoted exclusively to the subway," the first such units since the 1980s, whose "overall mission is counterterrorism and to fight crime"); Chicago Tribune, *Police Expanding Role in Fighting Terror*, REDEYE, Nov. 12, 2010, at 8 (reporting that the Chicago Police Department had widened its mission to include counterterrorism, hired a longtime FBI agent to create a counterterrorism and intelligence division within the department, and permanently assigned an officer to Washington, D.C., to liaise with federal agencies on counterterrorism); Jennifer Maloney, *Newest Dogged Pursuit*, NEWSDAY (New York), June 14, 2007, at A22 (reporting on the New York State Metropolitan Transit Authority's deployment of canine teams as part of counterterrorism efforts on the Long Island Rail Road, the nation's busiest commuter rail system); *Terrorism Preparedness Statement*, U. ARK. UNIV. POLICE, http://uapd.uark.edu/99.php (last visited Sept. 14, 2012) (describing terrorism preparations made by university police at the University of Arkansas, including the assignment of a full-time officer to the regional Joint Terrorism Task Force).

35. *E.g.*, Bradley Olson & Zain Shauk, *Smile, If You're Downtown*, HOUS. CHRON., Nov. 25, 2010, at A1 (describing a network of 250 to 300 surveillance cameras in downtown Houston); Vic Ryckaert, *Cameras Help Fight Crime, Police Say*, INDIANAPOLIS STAR, Dec. 31, 2007, at B1 (reporting on a 67-camera surveillance network in Indianapolis, as well as similar networks in Boston, Dallas, Los Angeles, and Chicago).

36. The New Jersey State Police, the New York Police Department, and the United States Secret Service each own SUVs, known as RadTrucks, that are outfitted with $200,000 worth of radiation detection equipment and used to patrol public highways for potential terrorist nuclear threats. *See* Sam Wood, *New SUVs Are Like Police Radar for Terrorism*, PHILA. INQUIRER, Sept. 9, 2007, at B10.

37. In Massachusetts, more than eighty cities and towns across the state have given their police officers access to military-grade assault rifles and other weaponry "in response to the fear of terrorist attacks." Donovan Slack, *Police Add Assault Rifles Across the State*, BOS. GLOBE, June 3, 2009, at A1. Notably, in Boston, the largest city in Massachusetts, Mayor Thomas Menino refused to issue any of the city's 200 assault rifles to neighborhood patrol officers after community leaders described the use of assault weapons as the "'militarization' of local police." *Id.* at A12.

38. In 2011, the Montgomery County Sheriff's Office, whose jurisdiction is north of Houston in Texas, used federal homeland security grant money to purchase an unmanned aerial vehicle for surveillance purposes. Robert Stanton, *Drones Prompt Privacy Fears*, HOUS. CHRON., Nov. 1, 2011, at B2; Stephen Dean, *New Police Drone Near Houston Could Carry Weapons*, CLICK2HOUSTON.COM, Nov. 10, 2011, http://www.click2houston.com/news/2

spent considerable time training officers how to respond to terrorist threats through classroom instruction, exercises, and, in some cases, public drills.[39] Finally—now more involved, better funded, better trained, and better equipped with the latest technology and weaponry than at any point during the last ten years[40]—local law enforcement agencies have sprung into action, providing heightened security[41] and heightened responses to potential terrorist threats.[42] Many of these

9619788/detail.html.

39. *See, e.g.*, Christine Byers, *Training Ground: Terrorist Attacks Lead to New Training for St. Louis County Police*, ST. LOUIS POST-DISPATCH, Sept. 28, 2011, at B1 (reporting on St. Louis County, Missouri, which in 2011 became the first county in the nation to require officers department-wide to undergo counterterrorism training); Tom Feeney, *Police Practice Derailing Terror Threats*, STAR-LEDGER (Newark, N.J.), Dec. 9, 2006, at 15 (describing a 150-officer rapid-response force designed to be activated in the aftermath of a terrorist attack, which was paid for with funding received from the Department of Homeland Security through the Urban Areas Security Initiative); Ann Scott Tyson, *Metro Stages a Display of Its Force*, WASH. POST, Feb. 3, 2010, at B2 (describing a mock "anti-terrorism sweep" conducted by Washington's Metro Transit Police during a weekday morning rush hour at the city's Union Station, which involved fifty officers armed with M-4 assault rifles and bomb-sniffing dogs).

40. *See supra* notes 33–39.

41. Police have become especially sensitive to individuals who act suspiciously near traditionally high-profile terrorist targets such as stadiums and airports. *See, e.g.*, Del Quentin Wilber, *Police on the Lookout for Terrorists With Missiles Near Airports*, WASH. POST, Sept. 9, 2006, at A3 (describing how Washington, D.C. area police forces patrol near airports to scout for terrorists with shoulder-fired rockets who may be looking to shoot down aircrafts during takeoffs and landings). Indeed, police have become so sensitive that such heightened responses are typical even when there is no evidence to connect the suspects to known terrorist groups, or even when the site in question is not directly targeted. *See* Charlie Cain & Francis X. Donnelly, *Michigan Quickly Enacts Emergency Plans*, DETROIT NEWS, Aug. 11, 2006, at 9A (describing how Michigan authorities, including state police, put emergency-response plans into action after British police reportedly foiled a plot by terrorists to explode planes bound for the U.S., despite the lack of evidence that any targets were in Michigan); Rebecca Lopez, *Figure in Airport Watch Case Confirms Terrorist Tie*, DALL. MORNING NEWS, Apr. 7, 2007, at 9B (reporting on two Muslim women in Dallas who became the subjects of a police intelligence bulletin after police observed them "acting suspiciously" at Love Field, though police also said they had no evidence the women were connected to terrorism, and one of the women had no criminal record).

42. For example, missing, stolen, or otherwise suspicious vehicles, which might have previously been treated as just that, now draw intense scrutiny from police out of concern for possible ties to terrorism. *See, e.g.*, Colleen Long, *Van Stirs Security Worries in NYC*, BOS. GLOBE, Dec. 31, 2009, at A8 (reporting on the New York Police Department's closure of Times Square after discovering a parked van without license plates in advance of New Year's Eve celebrations); Allison Steele, *Police Find Vans That Sparked Terror Alert*, PHILA. INQUIRER, Sept. 14, 2011, at B4 (describing how the theft of four rental trucks in Philadelphia, shortly before the tenth anniversary of the September 11 attacks, prompted a terrorism alert among city police). This is true even despite the occasional false alarm. *See, e.g.*, John M. Guilfoil, *Van's Fuel Sparks a Terrorism Response*, BOS. GLOBE, Oct. 17, 2011, at

responses are understandably colored by the terrorist attacks that have occurred in other countries during the years since the September 11 attacks.[43] But they have also become magnified in larger cities—especially New York City, where police are quick to increase security and implement emergency-response plans at major tourist centers when a terrorism alert arises almost anywhere in the world.[44] Clearly, police are going further than ever before to ensure that terrorists do not strike again. But in some cases, such as those in the next section, these efforts come at great expense to the civil liberties of those the police are trying to protect.

B. Local Law Enforcement's Expanded Role in Counterterrorism Has Raised Civil Liberties Concerns in the Past

Although the federal government was eager to enlist local law enforcement agencies as the "front line of defense" in the fight against terrorism,[45] this involvement has become a double-edged sword in the decade following September 11, 2001. In a number of incidents that have occurred during the last ten years, local law enforcement surveillance and intelligence-gathering activities conducted for counterterrorism purposes have drawn the attention of civil liberties advocates who say these activities infringe individuals' constitutional rights. This Part presents two of the most notable incidents from recent years, to provide a flavor of the types of activities with which this Comment is concerned.

B3 (reporting on a counterterrorism response by police in Tewksbury, Massachusetts, after an officer spotted two college students "who appeared to be of Middle Eastern descent" loading compressed natural gas into a van; it turned out the van was designed to run on natural gas as part of a harmless—albeit unlicensed—experiment with alternative fuels).

43. *See, e.g.*, Tom Hays, *Beneath NYC, Police Fight Terror with Stealth*, STAR-LEDGER (Newark, N.J.), Apr. 13, 2010, at 1 (describing how the NYPD has studied terrorist attacks on transit systems in Madrid, London, Bombay, and Moscow to develop best practices in defending the New York City Subway); Kevin Johnson & Thomas Frank, *Mumbai Attacks Refocus U.S. Cities*, USA TODAY, Dec. 5–7, 2008, at 1A (reporting on new precautions taken with "soft targets" by U.S. police forces following the November 2008 terrorist attacks in Mumbai, India).

44. Joie Tyrell, *Terror Plot Foiled in Britain*, NEWSDAY (New York), June 14, 2007, at A22 (describing how the NYPD strengthened security in the transit system and in major New York City tourist areas such as Times Square, Herald Square, and the theater district after police discovered a car bomb in a busy area of London).

45. *See supra* notes 24–25 and accompanying text.

1. Los Angeles Police Propose Mapping Muslim Communities (2007)

In 2007, the counterterrorism bureau of the Los Angeles Police Department (LAPD)[46] began developing a plan to identify and map Muslim enclaves[47] of Los Angeles.[48] The plan's ostensible purpose was "to help Muslim communities avoid the influence" of radical and extremist elements.[49] Under the plan, the LAPD would identify Muslim neighborhoods that were at risk of isolation using data from the U.S. Census Bureau[50] and demographic factors that, the police believed, made these neighborhoods susceptible to extremism and likely to become breeding grounds for homegrown terrorist cells.[51] Having identified these neighborhoods, the LAPD would then add information from community members about residents, homes, businesses, mosques, "language, culture, ethnic breakdown, socioeconomic status and [even]

46. As of 2010, the Los Angeles Police Department was the nation's third-largest loca law enforcement agency, with 9,858 sworn officers serving a population of 3.8 million residents. *Full-time Law Enforcement Employees by State by City, 2010*, FEDERAL BUREAU OF INVESTIGATION (2010), http://www.fbi.gov/about-us/cjis/ucr/crime-in-the-u.s/2010/crime-in-the-u.s.-2010/tables/10tbl78.xls/view (follow "Download Excel" hyperlink) [hereinafter *Full-time Law Enforcement*].

47. The metropolitan Los Angeles area—which includes Orange and Riverside Counties—has an estimated 500,000 Muslims, the second-largest Muslim community in the United States, after New York City's. Neil MacFarquhar, *Protest Greets Police Plan to Map Muslim Angelenos*, N.Y. TIMES, Nov. 9, 2007, at A23.

48. Richard Winton et al., *LAPD to Build Data on Muslim Areas*, L.A. TIMES, Nov. 9, 2007, at A1[hereinafter Winton, *LAPD to Build Data*] (quoting Deputy Chief Michael Downing of the Los Angeles Police Department, who was in charge of the Department's counterterrorism bureau at the time). The plan quickly became known in the media as a "mapping" plan, though Downing disputed this characterization, preferring instead the term "community engagement" plan. *Plan to Map L.A.'s Muslims Sparks Outrage*, NPR, 0:22–0:45 (Nov. 9, 2007), http://www.npr.org/templates/story/story.php?storyId=16162012 [hereinafter *Plan to Map*]. Perhaps ironically, however, the details of the plan first became public because of Downing's testimony before a United States Senate committee, in which he himself used the word "mapping." Michael P. Downing, Commanding Officer, Counter-Terrorism/Criminal Intelligence Bureau, L.A. Police Dep't., Statement Before the Committee on Homeland Security and Governmental Affairs, United States Senate 7 (Oct. 30, 2007) (prepared text available at http://www.lapdonline.org/assets/pdf/Michael%20 DowningTestimonyfortheU.S.Senate-Final.PDF).

49. Winton, *LAPD to Build Data*, *supra* note 48.

50. Richard Winton et al., *Outcry Over Muslim Mapping*, L.A. TIMES, Nov. 10, 2007, at A1 [hereinafter Winton, *Outrcy*]. *But see infra* note 62 and accompanying text.

51. Winton, *Outcry, supra* note 50. The same idea gained traction with police in New York City during 2007 as well, and likewise drew criticism from civil liberties groups. *See* Al Baker, *City Police Report Explores Homegrown Terrorism*, N.Y. TIMES, Aug. 16, 2007, at B3 (describing NYPD report that finds, among other things, "unassimilated Muslims in the United States are vulnerable to extremism").

social interactions" within the neighborhoods to paint a full picture of Muslim life in Los Angeles.[52] To perform this analysis, the LAPD partnered with the University of Southern California's National Center for Risk and Economic Analysis of Terrorism Events.[53] Although the LAPD said the program would not involve spying on citizens—comparing it instead to market research, and insisting the program would focus on groups, rather than individuals[54]—the LAPD's counterterrorism chief, Michael Downing, later testified before Congress that the program would use a "full-spectrum approach guided by an intelligence-led strategy."[55]

After the plan's details became public, the resulting uproar among civil liberties groups and Muslim activists was immediate.[56] Some groups compared the plan to "religious profiling,"[57] and the American Civil Liberties Union and community leaders expressed "grave concerns" about the plan's premise that "Muslims are more likely to commit violent acts than people of other faiths."[58]

The fallout was equally swift. The *Los Angeles Times*' editorial pages soon featured letters to the editor from non-Muslim readers generally condemning the plan.[59] Muslim groups also protested outside of the LAPD's headquarters building.[60] The LAPD's academic partnership with USC disintegrated as the university began distancing

52. Winton, *LAPD to Build Data*, *supra* note 48 (quoting Los Angeles Deputy Chief Michael P. Downing, who headed the LAPD's anti-terrorism bureau).

53. *Id.*

54. *Id.*

55. *Id.*; Downing, *supra* note 48, at 7.

56. Winton, *Outcry*, *supra* note 50. *But see* Winton, *LAPD to Build Data*, *supra* note 48 (quoting Salam Al-Marayati, the director of Los Angeles's Muslim Public Affairs Council, as saying Michael Downing, the LAPD's counterterrorism chief, is "well-known in the Muslim community" and has "been very forthright in his engagement with the Muslim community").

57. Winton, *Outcry*, *supra* note 50. *But see Plan to Map*, *supra* note 48, at 2:20–2:57 (interviewing the LAPD's counterterrorism chief, Michael Downing, who said that the police used criteria other than religious or racial characteristics in identifying Muslim enclaves at risk of extremism, though he did not identify the specific criteria that might be used).

58. Letter from Ranjana Natarajan, Staff Att'y, ACLU of S. Cal., et al., to Michael P. Downing, Commander, Counter-Terrorism/Criminal Intelligence Bureau, L.A. Police Dep't (Nov. 8, 2007), *available at* http://www.cair.com/Portals/0/pdf/Muslim_Leaders_to_LAPD.pdf.

59. *See* Margaret Manning et al., Letters to the Editor, *Is the LAPD Off the Map?*, L.A. TIMES, Nov. 13, 2007, at A18 (featuring four letters to the editor regarding the mapping plan, with three condemning the plan and one in favor).

60. Daniel B. Wood & Alison Tully, *Why L.A. Police Nixed Plan to Map Muslims*, CHRISTIAN SCI. MONITOR, Nov. 20, 2007, at 2.

itself from the project.[61] Experts, industry veterans, and Los Angeles residents alike expressed skepticism that the plan was even feasible, for at least four reasons: the Census Bureau may not compel Americans to disclose their religious affiliations;[62] Los Angeles neighborhoods are far from demographically homogenous;[63] surveys indicate American Muslims are more integrated and more dispersed than their European counterparts;[64] and decades of controversy over similar monitoring efforts by the FBI had convinced federal officials that it was best to avoid any initiatives with even the barest racial elements.[65] The LAPD initially stood behind the plan, but public criticism continued to mount, and less than a week after details of the plan became public, the LAPD announced it was cancelling the initiative.[66]

It is important to note that the LAPD canceled the initiative not because police concluded gathering intelligence on Muslim community members had no value,[67] but rather because of "widespread criticism by both Muslim and other religious leaders."[68] And though most community groups appeared satisfied by the LAPD's response to their protests,[69] civil liberties advocates remained suspicious, saying they

61. Richard Winton & Teresa Watanabe, *LAPD's Muslim Mapping Plan Killed*, L.A. TIMES, Nov. 15, 2007, at A1, A21 (reporting that "after details of the effort were made public last week, USC officials said they were carefully studying whether to join the endeavor and stressed that no deal had been made").

62. *See* 13 U.S.C. § 221(c) (2006) ("Notwithstanding any other provision of this title, no person shall be compelled to disclose information relative to his religious beliefs or to membership in a religious body."). This statute has been in place since 1976. Act of Oct. 17, 1976, Pub. L. No. 94-521, § 13, 90 Stat. 2465.

63. *See* Winton, *Outcry*, *supra* note 50.

64. *Id.*

65. *Id.*

66. Greg Krikorian & Teresa Watanabe, *Experts See Value in Data on Muslims*, L.A. TIMES, Nov. 16, 2007, at B1, B10.

67. On the contrary, veteran counterterrorism experts and academics said that the data would have been valuable both in the abstract and that there was precedent to indicate the data would have value in a pragmatic sense. *Id.* As one retired counterterrorism official put it, "In the old days, when you looked for La Cosa Nostra, you didn't start looking in Polish neighborhoods." *Id.*

68. Wood & Tully, *supra* note 60.

69. Los Angeles Police Chief William Bratton met for two hours with Muslim community leaders to hear their concerns before giving a public speech in which he declared the mapping project was "DOA—dead on arrival." Krikorian & Watanabe, *supra* note 66. It is worth noting that, throughout the period of public outcry over the plan, both Chief Bratton and Deputy Chief Downing were generally well regarded by the city's Muslim community for their willingness to hear the community's concerns and their generally progressive views on community policing. *See* MacFarquhar, *supra* note 47 ("Among those [members of the

would continue to monitor the LAPD's activities in this area going forward.[70]

The civil liberties advocates may have had good reason to remain suspicious. The epilogue to the mapping initiative is that, in 2008, the LAPD launched a new program in which it modified the investigative-report form that all officers must complete in response to a crime, adding a section to the form for officers to describe activities they have witnessed that may be related to terrorism.[71] If an officer reports such information, the report is forwarded to the LAPD's counterterrorism bureau, where it is entered into the LAPD's database for further analysis—both by the LAPD itself and other law enforcement agencies.[72] But the LAPD's officers are required to report such activities *even if* the activities are not connected to criminal activity and *even if* the officer lacks any independent suspicion of wrongdoing.[73] Furthermore, the ACLU noted many of the activities considered "suspicious" by the LAPD were innocuous and commonplace.[74] Despite these concerns, the LAPD's suspicious-activity reporting model has not only become cemented within the department,[75] but has also been adopted in at least a dozen other cities—where, so far, the only results

---

Muslim community] interviewed, whatever their position on the project, Mr. Downing rated high marks for his community policing efforts . . . ."); Wood & Tully, *supra* note 60 (quoting a police accountability advocate as describing Bratton as "one of America's finest" police chiefs).

70. Wood & Tully, *supra* note 60 (quoting an ACLU attorney who mentions the LAPD's "long history . . . of profiling" and that the group will "make sure that it[—]this profiling[—]comes to an end").

71. Josh Meyer, *LAPD Leads the Way in Local Counter-Terrorism*, L.A. TIMES, Apr. 14, 2008, at B4.

72. *Id.*

73. Special Order, William J. Bratton, Chief of Police, L.A. Police Dep't., No. 11 on Reporting Incidents Potentially Related to Foreign or Domestic Terrorism (Mar. 5, 2008), *reprinted in* FINDINGS AND RECOMMENDATIONS OF THE SUSPICIOUS ACTIVITY REPORT (SAR): SUPPORT AND IMPLEMENTATION PROJECT, 36–42 (2008), *available at www.it.ojp.gov/documents/SAR_Report_October_2008.pdf*.

74. MIKE GERMAN & JAY STANLEY, AM. CIVIL LIBERTIES UNION, FUSION CENTER UPDATE 1–2 (2008), *available at* http://www.aclu.org/pdfs/privacy/fusion_update_20080729.pdf. Examples included "taking measurements," "using binoculars," and "taking pictures or video footage 'with no apparent esthetic value.'" *Id.* at 2. The report also cited several examples in which local law enforcement agencies across the country had temporarily detained or interrogated individuals for engaging in activities similar to these. *Id.* at 6–7.

75. Los Angeles Police Chief William Bratton has described the program as the "'heart and soul' of the LAPD's counterterrorism efforts." Siobhan Gorman, *LAPD Terror-Tip Plan May Serve as Model*, WALL ST. J., Apr. 15, 2008, at A3.

from these reports have been non-terrorism-related arrests.[76]

In many ways, the new program closely resembles (and achieves many of the same objectives as) the abandoned plan to map Muslim neighborhoods—it involves a comprehensive effort to gather and analyze data about everyday activities—but without a sensitive racial or religious component. In fact, such intelligence gathering and surveillance remains one of the most common ways in which local law enforcement agencies have begun to encroach upon civil liberties in the name of counterterrorism in the years following September 11, 2001.[77]

2. New York City Police Infiltrate Muslim Neighborhoods (2001–present)

Not long after the terrorist attacks of September 11, 2001, the New York Police Department (NYPD)[78] established a secret intelligence unit designed to gather information on Muslim and other ethnic neighborhoods in New York City as the first step toward preventing future terrorist attacks on the city.[79] The unit,[80] which still operates as of

---

76. *See* Eric Schmitt, *Surveillance Effort Draws Civil Liberties Concern*, N.Y. TIMES, Apr. 29, 2009, at A12 (reporting that the LAPD program has also been implemented in Boston, Chicago, Houston, Las Vegas, Miami, Phoenix, Seattle, and Washington, D.C., as well as in Florida, Virginia, and New York State, with hopes for a national network to be in place by 2014; none of the city officials interviewed for the article could name any examples of potential terrorist attacks that had been stopped as a result of the program).

77. *See* JEROME P. BJELOPERA, CONG. RESEARCH SERV., R40901, TERRORISM INFORMATION SHARING AND THE NATIONWIDE SUSPICIOUS ACTIVITY REPORT INITIATIVE: BACKGROUND AND ISSUES FOR CONGRESS 2 (2011) (noting that "[a]lthough data mining for counterterrorism purposes predated the 9/11 attacks, it was considered a particularly promising tool after it was learned that certain database searches would have disclosed connections between . . . two 9/11 hijackers who were on a government terrorist watch list prior to September 11" (footnote omitted)).

78. In 2010, the New York Police Department was the nation's single largest city law enforcement agency, with 34,817 sworn officers serving a population of 8.3 million. *Full-time Law Enforcement*, *supra* note 46.

79. *See* Matt Apuzzo & Adam Goldman, *NYPD Spies in Jersey*, STAR-LEDGER (Newark, N.J.), Aug. 25, 2011, at 1 [hereinafter Apuzzo & Goldman, *NYPD Spies*].

80. In its current form, the NYPD's intelligence unit is the brainchild of David Cohen, a retired CIA official who was hired specifically to turn the unit into a localized version of the CIA. *Id.* at 5. Prior to Cohen's tenure, the NYPD's intelligence unit was apparently best known for driving foreign diplomats around New York City. *Id.* City officials instead wanted a unit that would "analyze intelligence, run undercover operations and cultivate a network of informants." *Id.* Cohen was just the man for the job—he brought aboard former colleagues from his days at the CIA to train NYPD officers in the art of intelligence gathering. *Id.* Cohen also convinced a federal judge to allow police officers to open investigative files without any suspicion of criminal activity, lifting "major elements" of restrictions that had

2012,[81] infiltrates these neighborhoods using undercover officers and informants as well as information-gathering and mapping techniques similar to those proposed for the earlier LAPD plan.[82]

As part of the NYPD intelligence unit's activities, undercover officers[83] from the unit monitor ethnic communities,[84] either directly or through the use of informants[85] who attend local mosques and gather information from weekly sermons to Muslim communities.[86] Using these techniques, the officers have infiltrated dozens of mosques and analyzed hundreds of them.[87] NYPD officers file daily reports on innocuous behavior they observe at cafés, restaurants, and other public locations.[88] They also talk to "store owners to determine their ethnicities and gauge their views" and join clubs and cricket teams in ethnic neighborhoods.[89] And just as the LAPD had intended to do with

---

been in place since 1985. *See* David A. Harris, *Law Enforcement and Intelligence Gathering in Muslim and Immigrant Communities After 9/11*, 34 N.Y.U. REV. L. & SOC. CHANGE 123, 151 (2010); Apuzzo & Goldman, *NYPD Spies*, *supra* note 79; *see also* Chris Hawley, *Barbara Handschu Likens NYPD Syping on Muslims to Spying on Free Speech Advocates*, HUFFINGTON POST (New York), Nov. 17, 2011, http://www.huffingtonpost.com/2011/11/17/in-nypd-spying-a-yippie-l_n_1099479.html (stating that "Cohen . . . asked Judge Charles Haight to loosen the Handschu rules" just "[o]ne day after the first anniversary of the attacks"). The unit now employs "16 officers speaking at least five languages, [and] is the only squad of its kind known to be operating in the country." Matt Apuzzo & Adam Goldman, *Documents: NYPD Spied on Area Muslims' Ordinary Lives*, STAR-LEDGER (Newark, N.J.), Sept. 1, 2011, at 5 [hereinafter Apuzzo & Goldman, *Documents*].

81. *See, e.g.*, Michael Powell, *In a Post-9/11 City, a Person's Language Can Be a Cause for Police Suspicion*, N.Y. TIMES, Aug. 28, 2012, at A17 (describing activities conducted by the NYPD's intelligence unit "earlier this summer" in 2012, such as "eavesdropp[ing] on thousands of conversations between Muslims in restaurants and stores in New York City and New Jersey and on Long Island").

82. Apuzzo & Goldman, *NYPD Spies*, *supra* note 79.

83. Undercover officers became known as "rakers," following a comment from Cohen to his subordinates that he wanted the unit to "rake the coals [of New York City], looking for hot spots." *Id.* at 5.

84. *Id.* at 1, 5. Officers are matched to ethnic neighborhoods using data from the U.S. Census Bureau—a process that prompted officers to begin calling the unit the "Demographic Unit." *Id.* at 5.

85. Officers recruited informants by arresting them for outstanding warrants or traffic violations, and then using the arrests as leverage. Chuck Bennett, *NYPD Has Shadowy Spy Guys*, N.Y. POST, Aug. 25, 2011, at 12.

86. Apuzzo & Goldman, *NYPD Spies*, *supra* note 79.

87. Kimberly Dozier & Matt Apuzzo, *CIA Probing Legality of Its Work with NYPD: Agency Helped Undercover Cops Spy on Muslim Communities*, STAR-LEDGER (Newark, N.J.), Sept. 14, 2011, at 3.

88. *See id.*

89. Chris Hawley, *Muslim Leaders: NYPD Spying Wrecks Mayor's Goodwill*, STAR-

its now-abandoned mapping plan, the NYPD uses this information—along with a list of "ancestries of interest"—to map the metropolitan area's ethnic neighborhoods.[90] The surveillance and intelligence gathering that officers perform for the unit's investigations even occasionally takes them beyond the city limits.[91]

After the program became public,[92] the NYPD, the CIA, and New York City officials began the elaborate dance of denying the most controversial elements of the program, such as racial profiling,[93] while asserting that police needed to do everything within their power to protect the city from future attacks.[94] As with the LAPD's mapping plan, it was not long before the tide of public opinion began to turn against the program.[95] But unlike in Los Angeles, officials in New York City were not so quick to scrap the program, perhaps because the memories of September 11, 2001, were more vivid closer to the site of the terrorist attacks.[96] City Council members questioned New York

---

LEDGER (Newark, N.J.), Dec. 30, 2011, at 29.

90. Apuzzo & Goldman, *Documents*, *supra* note 80. The so-called "ancestries of interest" are from twenty-eight countries, "nearly all [of which are] heavily Muslim"—though the mayor of New York City, Michael Bloomberg, asserted that the NYPD does not factor religion into policing tactics. *Id.*

91. According to some reports, NYPD intelligence officers have operated as far afield as New Jersey, upstate New York, Pennsylvania, Connecticut, and Massachusetts. *See, e.g.*, *id.*; Bennett, *supra* note 85.

92. The program became public through a series of investigative reports by the Associated Press. *See, e.g.*, Apuzzo & Goldman, *Documents*, *supra* note 80.

93. *NYPD Confirms CIA Advisory Role on 'Trade Craft Issues*,' USA TODAY, Aug. 26, 2011, http://www.usatoday.com/news/washington/story/2011-08-26/NYPD-confirms-CIA-advisory-role-on-trade-craft-issues/50143402.

94. Apuzzo & Goldman, *NYPD Spies*, *supra* note 79. Some, such as CIA spokesperson Jennifer Youngblood, portrayed the CIA–NYPD partnership as matter-of-fact ("'It should not be a surprise to anyone that, after 9/11, the Central Intelligence Agency stepped up its cooperation with law enforcement on counterterrorism issues or that some of that increased cooperation was in New York . . . .'"), while others, such as NYPD spokesperson Paul Browne, were literally unapologetic ("'The New York Police Department is doing everything it can to make sure there's not another 9/11 here and that more innocent New Yorkers are not killed by terrorists . . . . And we have nothing to apologize for in that regard.'"). *Id.*

95. *See id.* (reporting that "the Council on American–Islamic Relations, a leading Muslim civil rights organization, called on the Justice Department to investigate"); Adam Goldman & Eileen Sullivan, *N.Y. Police Build Database of Immigrant Life*, STAR-LEDGER (Newark, N.J.), Sept. 23, 2011, at 2 (reporting that state Representative Rush Holt has also urged the U.S. Justice Department to investigate the NYPD's program); Hawley, *supra* note 89 (reporting that Islamic religious and civic leaders feel that the NYPD surveillance program has cost Mayor Michael Bloomberg the goodwill he generated by supporting a controversial Islamic center near the World Trade Center site).

96. *See generally* Jesse Washington, *In N.Y., Taking Surveillance in Stride*, STAR-

Police Commissioner Ray Kelly about the program at a hearing in October 2011,[97] but were apparently satisfied with Kelly's assertions that the program is lawful. Through the middle of 2012, various civil liberties groups continued to speak out against the program, and a Muslim civil rights group filed a lawsuit to restrain the NYPD's intelligence unit from spying on Muslims[98]—but, in the interim, city officials have not yet taken any action against the unit.[99]

Adding fuel to the fire of controversy, later reports indicated the NYPD program has so far had only mixed success. In a high-profile defense of the NYPD, Representative Peter King of New York asserted that the surveillance had stopped at least fourteen "terror plots" in New York City since September 11, 2001.[100] But a closer review of the cases cited by Representative King revealed that many of the plans "may never have existed," or may have included "plots the NYPD had little or no hand in disrupting."[101] The program's surveillance efforts were hit-and-miss too,[102] and the program has put a strain on the relationship

---

LEDGER (Newark, N.J.), Nov. 13, 2011, at 11 (interviewing New Yorkers who express "ambivalence" about police surveillance, weighing the "competing impulses of civic welcome and civic safety").

97. Joseph Goldstein, *City Council Grills Kelly on Police Surveillance of Muslims*, N.Y. TIMES, Oct. 7, 2011, at A23.

98. Eileen Sullivan, *Muslims File Federal Suit to Stop NYPD Spying*, HUFFINGTON POST, June 6, 2012, http://www.huffingtonpost.com/2012/06/06/nj-muslims-file-federal-s_0_n_1574019.html. The lawsuit, filed in June 2012, named eight New Jersey-based Muslims as plaintiffs and is supported by Muslim Advocates, a civil rights advocacy group headquartered in California. *Id.* The lawsuit was the first to be filed against the NYPD. *Id.* At the time of the filing, however, a number of government officials, including the New Jersey State Attorney General and the Obama administration's top counterterrorism advisor, had examined the NYPD program and concluded it was not breaking any laws. *Id.*

99. *See NYPD Confirms CIA Advisory Role on 'Trade Craft Issues*,*' supra* note 93.

100. *Rep. King Demands "Uninformed" Members of Congress Stop Smearing the NYPD*, UNITED STATES HOUSE OF REPRESENTATIVES (Dec. 15, 2011), http://www.house.gov/apps/list/hearing/ny03_king/stopnypdsmear.html. The attacks supposedly foiled included plans to destroy the Brooklyn Bridge; flood the Holland and Lincoln Tunnels, which cross under the Hudson River from New Jersey to New York City; and bomb the city's Herald Square subway station. *See* David Morgan, *Other Foiled NYC Terror Plots Since 9/11*, CBSNEWS.COM (Nov. 21, 2011, 10:28 AM), http://www.cbsnews.com/8301-201_162-57328623/other-foiled-nyc-terror-plots-since-9-11/.

101. Matt Apuzzo et al., *NYPD's Spying Programs Yielded Only Mixed Results*, SAN DIEGO UNION-TRIB., Dec. 23, 2011, http://www.utsandiego.com/news/2011/dec/23/nypds-spying-programs-yielded-only-mixed-results/. The attempted bombing of the Herald Square subway station in 2004 was the only attack that journalists could confirm had been prevented by the NYPD program. *Id.*

102. The NYPD identified several fringe groups within the Muslim community, but failed to identify certain radical members within those organizations; large amounts of data

between Muslim communities in New York and police, arguably hampering the NYPD's ability to leverage local knowledge to its advantage.[103] But the specter of another terrorist attack looms large in New York City, and the resulting "sense of national vulnerability" has enabled the program to continue operating.[104] At the same time, many of the news reports detailing the NYPD intelligence program—like the LAPD's mapping plan before it—expressed a certain breathless shock that such widespread surveillance could happen in America, tiptoeing around the central question: How could this happen?

III. THE FOURTH AMENDMENT OFFERS LITTLE PROTECTION AGAINST POLICE SURVEILLANCE AND INTELLIGENCE GATHERING

Among the many constitutional provisions that protect individuals from unwanted government intrusions into their day-to-day lives—and perhaps the provision that has the most direct relevance to law enforcement, criminal investigations, and surveillance—is the Fourth Amendment. This Part will first discuss the historical development of the Amendment, which will help to illuminate why the police surveillance and intelligence-gathering activities described in the previous Part raise constitutional issues. This Part then discusses three relevant exceptions to the Amendment's general rule, which illustrate why many of the investigative tactics police use as part of their intelligence operations are exempt from the Amendment's protections, and, from a constitutional perspective, generally continue unabated.

A. An Overview of the Fourth Amendment

By its own terms, the Fourth Amendment only protects against "unreasonable searches and seizures,"[105] and the Supreme Court has historically held that, at least within the criminal context, a search or

were gathered about entirely innocent people; and one investigative tactic—monitoring everyone in New York City who legally changed names—produced no results at all. *Id.*

103. *See id.* (describing how some Islamic leaders have counseled residents to avoid reporting extremist, anti-American talk to the police because the person doing the talking is likely a police informant); *see also* Harris, *supra* note 80, at 130 (describing how police use of informants in Muslim neighborhoods "will cause lasting damage to efforts to bring Muslim communities and law enforcement together to build a common cause against extremism").

104. David Crary, *9/11 Paranoia Gives Way to Fears That We've Gone Too Far*, STAR-LEDGER (Newark, N.J.), Nov. 20, 2011, at 6 (quoting Donna Lieberman, a spokesperson for the New York Civil Liberties Union).

105. U.S. CONST. amend. IV.

seizure is generally unreasonable if it is conducted without a warrant,[106] subject to certain exceptions.[107] The Amendment also prohibits the issuance of warrants without probable cause,[108] a restriction that is important with respect to widespread police surveillance and intelligence gathering because "searches" include not only physical searches of premises and persons, but also, under certain circumstances, the surveillance of individuals, or even the collection of information.[109] As we have seen, a great deal of the counterterrorism-related intelligence gathering conducted by police in the years since September 11, 2001, has lacked probable cause.[110] While this might appear to indicate that such intelligence gathering—and any evidence gleaned from it—is barred by the Fourth Amendment,[111] a brief survey of the Amendment's history reveals that there are a number of exceptions to the Amendment's rule that allow police to conduct these operations without constitutional consequence.

B. Historical Development of the Fourth Amendment

Although the Fourth Amendment was inspired by a lively period of revolution and political protest,[112] it received little attention in

106. *See* Katz v. United States, 389 U.S. 347, 357 (1967) (holding that, with respect to the Fourth Amendment, a search is unreasonable when it is "conducted outside the judicial process, without prior approval by judge or magistrate").

107. The relevant exceptions are discussed later in this Part. There are many other exceptions that are not discussed in this Comment, primarily because they either apply outside of the criminal context or because they have no application to surveillance and intelligence gathering. *See infra* Part III.C.

108. U.S. CONST. amend. IV.

109. *Katz*, 389 U.S. at 353 (holding that "the Fourth Amendment governs not only the seizure of tangible items, but extends as well to the recording of oral statements . . . the Fourth Amendment protects people—and not simply 'areas'—against unreasonable searches and seizures").

110. *See supra* Part II.B.

111. The primary method by which the Fourth Amendment's protections are enforced is the so-called exclusionary rule, which prohibits the government from using evidence that was obtained through a search or seizure that violates the Amendment; this rule was established in *Weeks v. United States*, 232 U.S. 383, 392, 398 (1914). In 1961, the Supreme Court decided in *Mapp v. Ohio* that the Fourth Amendment—and with it, the exclusionary rule—also applied to state governments by way of the Fourteenth Amendment's Due Process Clause. 367 U.S. 643, 655 (1961).

112. The Fourth Amendment's origins can be traced to the writs of assistance, or general search warrants, frequently used by authorities in Great Britain's American colonies. Rachael A. Lynch, Note, *Two Wrongs Don't Make a Fourth Amendment Right:* Samson *Court Errs in Choosing Proper Analytical Framework, Errs in Result, Parolees Lose Fourth*

constitutional jurisprudence for most of its first 100 years.[113] It was not until *Boyd v. United States*, in 1886,[114] that it became clear the Amendment protected individuals from unwarranted government intrusions upon their private property.[115] From the time *Boyd* was decided until 1928, however, the Fourth Amendment was limited in that it only protected the "physical invasion of a protected space"[116]—and the Court's strict adherence to this principle unwittingly set in motion events that would lead to our modern conception of the Fourth Amendment.

In 1928, the Court decided the landmark case of *Olmstead v. United States*,[117] in which federal agents—without a warrant—used a telephone wiretap over several months to discover that Olmstead and his colleagues were conspiring to distribute liquor in violation of the National Prohibition Act.[118] The Court refused to grant Olmstead the Fourth Amendment's protections, distinguishing his case—where there was no physical intrusion of the premises—from past cases where there

---

Amendment Protection, 41 AKRON L. REV. 651, 654 (2008). Authorized by the Townshend Revenue Act, 1767, 7 Geo. 3, c. 46 (Eng.), the writs allowed royal customs agents "to enter and go into any House, Warehouse, Shop, Cellar, or other Place, in the British Colonies or Plantations in *America*" as part of their duties. The writs were most famously used in the case of *Wilkes v. Wood*, (1763) 98 Eng. Rep. 489 (K.B.) 489, in which a printer responsible for a pamphlet critical of King George III became the target of one of the writs—as well as a cause célèbre among the American colonists and one of the most significant influences on the drafting of the Fourth Amendment. *See* Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 772 & nn.53–54 (1994).

113. Justin F. Marceau, *The Fourth Amendment at a Three-Way Stop*, 62 ALA. L. REV. 687, 700 (2011). Possible reasons for this might be that the Fourth Amendment did not yet apply against the states; and there were few federal crimes. *Id.* at 701.

114. Boyd v. United States, 116 U.S. 616 (1886).

115. In *Boyd*, the Court considered the constitutionality of a series of laws that had been passed in the 1860s and 1870s. *Id.* at 621. The laws allowed the government to file an affidavit alleging a defendant had violated "any of the revenue laws of the United States," and thus compel the defendant to produce related financial documents to help the government prove its case; if the defendant did not comply, the court would accept the allegations as true. *Id.* at 619–20. Although the government argued that there is no search or seizure when the defendant is the one producing the documents, *id.* at 621, the Court shrewdly noted that the law's guilt-by-default setup offered defendants little practical choice in the matter. *Id.* at 621–22. Thus, the Court declared, the government's invasion of "personal security, personal liberty and private property" ran afoul of the Amendment's protections. *Id.* at 630.

116. Vivek Kothari, *Autobots, Decepticons, and Panopticons: The Transformative Nature of GPS Technology and the Fourth Amendment*, 6 CRIM. L. BRIEF 37, 38 (2010).

117. Olmstead v. United States, 277 U.S. 438 (1928).

118. *Id.* at 455–57.

was an "actual entrance into the private quarters of the defendant."[119] The Court bluntly concluded: "The Amendment does not forbid what was done here. There was no searching . . . . The evidence was secured by the use of the sense of hearing and that only. There was no entry of the houses or offices of the defendants."[120] The Court thus staked itself to its rule that the Amendment protected against government intrusions only in the case of intrusions into physical premises, and, in the process, ensured the Amendment "was not an evolving instrument of privacy protection"—especially with respect to new technologies.[121]

Four decades later, perhaps recognizing that "the continuing vitality of *Olmstead* was in serious doubt,"[122] the Court finally put the physical-premises rule to bed. In 1967, the Court decided *Katz v. United States*,[123] ushering in the modern era of Fourth Amendment jurisprudence.[124] In *Katz*, police suspected the defendant of violating the Wire Act,[125] and, as part of their investigation, eavesdropped on Katz's telephone calls without a warrant.[126] As a result of the evidence police obtained through this warrantless surveillance, Katz was found guilty on all counts.[127] Katz appealed his conviction to the Supreme Court, asking the Court to

---

119. *Id.* at 464.

120. *Id.* There was no entry into the defendants' houses or offices because the government had attached its wiretap to external telephone wires leading into the buildings. *Id.* at 457.

121. Marceau, *supra* note 113, at 703–04; *see also* Berger v. New York, 388 U.S. 41, 49 (1967) ("The law, though jealous of individual privacy, has not kept pace with these [electronic eavesdropping] advances in scientific knowledge.").

122. Nathan Petrashek, Comment, *The Fourth Amendment and the Brave New World of Online Social Networking*, 93 MARQ. L. REV. 1495, 1516 (2010). As the Supreme Court noted in *Berger*, the tide began to turn against *Olmstead* and its progeny in 1963, when the Court recognized for the first time in *Wong Sun v. United States*, 371 U.S. 471, 485 (1963), that "verbal evidence may be the fruit of official illegality under the Fourth Amendment." 388 U.S. at 52.

123. Katz v. United States, 389 U.S. 347 (1967).

124. *See* Kothari, *supra* note 116, at 38–39 (providing a brief history of the Fourth Amendment jurisprudence, which summarizes *Katz* as the last case that led to the "modern search and seizure doctrine").

125. The Wire Act prohibits the interstate transmission by wire of information involving bets or wagers. 18 U.S.C. § 1084(a) (2006).

126. FBI agents attached microphones to the tops of two out of three telephone booths in a bank of three booths that Katz was known to use; the third booth was disabled by the telephone company. Katz v. United States, 369 F.2d 130, 131 (9th Cir. 1966). The agents then watched the phone booths, and activated the microphones whenever Katz was in one of the booths—enabling them to obtain a record of Katz's end of the phone calls, which involved "the placing of bets and the obtaining of gambling information" by Katz. *Id.*

127. *Id.*

determine "[w]hether physical penetration of a constitutionally protected area is necessary before a search" violates the Fourth Amendment's protections.[128] But the Court, led by Justice Stewart, discarded Katz's formulation of the issue, almost matter-of-factly asserting instead that "the Fourth Amendment protects people, not places."[129] The Court acknowledged that *Olmstead* could "no longer be regarded as controlling," and that the evidence obtained by means of the wiretap was inadmissible because it was obtained without a warrant.[130]

Although Justice Stewart's majority opinion invalidated the *Olmstead* line of case law, it never established a clear rule subsequent courts might use in place of *Olmstead*.[131] Instead, later courts have followed the standard laid out by Justice Harlan in his concurring opinion,[132] in which he agreed with the majority that the Amendment protects "people, not places," but asserted that its protections could only be invoked if a two-part test was satisfied: "[F]irst that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[133]

Justice Harlan's test—whether the defendant had a "reasonable expectation of privacy"—has become, for better or for worse, the modern standard for Fourth Amendment jurisprudence.[134] In what might be seen as an improvement over the *Olmstead* standard, *Katz* rejects stagnation[135] and is "inherently non-static[,] . . . derived from evolving social norms, practices, and expectations."[136] But the Court's increasing focus on reasonableness has also meant the Court has found that, under certain circumstances, an individual's expectation of privacy was *not* reasonable—and thus that law enforcement was able to carry

128. *Katz*, 389 U.S. at 350.

129. *Id.* at 348–51. The Court famously went on: "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. . . . But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." *Id.* at 351–52 (citation omitted).

130. *Id.* at 353, 356–57.

131. Kothari, *supra* note 116, at 39.

132. *Id.*

133. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

134. Marceau, *supra* note 113, at 705.

135. *Id.* at 710.

136. *Id.* at 705.

out actions that might otherwise offend the Fourth Amendment.[137] Indeed, many of the police activities conducted as part of the widespread surveillance and intelligence gathering operations described in Part II fall into these gaps in the Amendment's protections.[138] In short, "the shifting meaning of the Fourth Amendment that was adopted in *Katz* has come to be seen as a threat as well as a benefit to civil liberties."[139] This Comment addresses three of these exceptions in the following section.

C. Exceptions to the Fourth Amendment's General Rule

1. Public Vantages

Before *Katz*, when the Fourth Amendment still only protected physical spaces, rather than individuals, courts had long recognized that "the eye cannot . . . be guilty of a trespass."[140] And though the core Fourth Amendment doctrine has since undergone various twists and turns, the Court has consistently held that, as long as police are "lawfully present at a location," visual surveillance is generally not a "search" within the context of the Amendment, and therefore does not invoke its protections.[141] This is true even though technology and police tactics have greatly improved law enforcement's ability to conduct visual surveillance,[142] such that today there are still only two categories of cases where the Court has limited the scope of the public-vantage exception: (1) cases in which law enforcement's use of surveillance technology allows officers to "exceed" normal levels of perception,[143] and (2) cases

137. *See infra* notes 180–85 and accompanying text.

138. See *infra* Part III.C (discussing three of the exemptions to the Fourth Amendment's General Rule—public vantages, assumption of the risk, and third parties).

139. *Id.* at 138.

140. Boyd v. United States, 116 U.S. 616, 628 (1886).

141. *See* Thomas K. Clancy, *What Is a "Search" Within the Meaning of the Fourth Amendment?*, 70 ALB. L. REV. 1, 22–23 & n.134 (2006) (noting that the principles underlying the idea that visual inspections are not searches date to 1765). This has remained largely true, even though the Court has subsequently been actively involved in deciding visual surveillance cases. *See* Marissa A. Lalli, Note, *Spicy Little Conversations: Technology in the Workplace and a Call for a New Cross-Doctrinal Jurisprudence*, 48 AM. CRIM. L. REV. 243, 271 (2011) (noting that, post-*Katz*, the Court "became increasingly concerned" with methods that law enforcement used to gather information about the subjects of its surveillance).

142. *See* Clancy, *supra* note 141, at 33 (noting that the Court's "cautions and concerns about [new technologies] . . . have rarely been translated into labeling the employment of the technology . . . as a search").

143. *See* Kyllo v. United States, 533 U.S. 27, 40 (2001); *see also* Andrew Riggs Dunlap,

in which law enforcement relies on technology that is not in "general public use."[144]

The first category—ruling out surveillance technology that allows officers to exceed normal levels of visual perception—might seem to disqualify most applications of the public-vantage doctrine altogether. But the Court has been careful to distinguish between those technologies that *exceed* normal levels of perception and those that merely *enhance* perception, restricting only the former while still allowing the latter.[145] In fact, the Court has drawn the line between enhancing and exceeding normal levels of perception such that a great deal of surveillance technology is still constitutionally permissible.[146] As

---

Note, *Fixing the Fourth Amendment with Trade Secret Law: A Response to* Kyllo v. United States, 90 GEO. L.J. 2175, 2181–84 (2002) (discussing the Court's concerns with sense exceeding technology absent concerns about public use of the equipment).

144. Kyllo, 533 U.S. at 40.

145. *See* Dunlap, *supra* note 143, at 2183 ("Technologies that allowed the government to 'see' more clearly did not offend the Fourth Amendment."). A famous pair of Fourth Amendment cases illustrates the difference between enhancing and exceeding normal levels of perception. In *United States v. Knotts*, the Court allowed police to track a criminal suspect to his secret lair using a radio beeper hidden in a drum of chemicals the suspect was transporting. 460 U.S. 276, 278 (1983). The Court said that no constitutional issues were involved, because the police could have just as easily used visual surveillance to track the suspect. *Id.* at 285. In *United States v. Karo*, however, police used a similar radio beeper to track the movements of a container of ether inside of a home; the Court held this was a search because "the police used the beeper to 'see' what they could not see unaided." Lalli, *supra* note 141, at 272 (citing United States v. Karo, 468 U.S. 705, 714, 719–21 (1984)).

The wrench in the works is the Supreme Court's recent decision in *United States v. Jones*, in which it held the use of a GPS device to track a criminal suspect's vehicle amounted to a search protected by the Fourth Amendment. United States v. Jones, 132 S. Ct. 945, 949 (2012). In *Jones*, police attached a GPS device to the bottom of the vehicle Jones was driving and tracked the vehicle for four weeks; the government later used this evidence to convict Jones of various drug-related crimes. *Id.* at 948. The Court distinguished *Jones* from *Knotts* and *Karo*, writing that in the two earlier cases, the defendants accepted the GPS device into their possession (albeit unknowingly), while in *Jones*, the police placed the device directly onto Jones's vehicle. *Id.* at 952. At the core of this analysis is the Court's insistence that *Katz*'s "reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the [pre-*Katz*] common-law trespassory test." *Id.* Commentators were quick to seize on the Court's decision in *Jones* as a "signal event in Fourth Amendment history"—though it may take some time before we fully understand whether, and how, it alters the analysis here. Adam Liptak, *Justices Reject GPS Tracking in a Drug Case*, N.Y. TIMES, Jan. 24, 2012, at A1.

146. *See, e.g.*, Dow Chem. Co. v. United States, 476 U.S. 227, 238–39 (1986) (allowing the use of an aerial surveillance camera and photographic magnification that could detect "wires as small as 1/2-inch in diameter"); California v. Ciraolo, 476 U.S. 207, 215 (1986) (upholding federal agents' airplane surveillance of the defendant's marijuana crop from an altitude of 1,000 feet); Texas v. Brown, 460 U.S. 730, 739–40 (1983) (ruling that a police officer who shined a flashlight into a stopped car "trenched upon no right secured to the

a result, this is not quite the broad restriction it may have initially appeared to be.

The second category in which the Court has said police cannot rely on the public vantage doctrine—when their surveillance employs technology that is not in general public use[147]—finds its rationale in *Katz*'s rule that the Fourth Amendment protects defendants who have a "reasonable expectation of privacy."[148] But while this rule may appear fair in principle—defendants cannot be expected to take measures to protect their privacy against modes of intrusion of which they are unaware—it is also limited in practice.[149] For as soon as defendants gain awareness of a certain type of technology, the implication is that "they are [then] responsible for protecting themselves from its possible invasions."[150]

Clearly, when it comes to widespread surveillance and intelligence gathering, the public-vantage doctrine is an enormous asset for law enforcement; even taking into account the limits described here, police may still conduct virtually unlimited visual surveillance of their subjects without offending the protections offered by the Fourth Amendment.

[defendant] by the Fourth Amendment"); On Lee v. United States, 343 U.S. 747, 754 (1952) (allowing the "use of bifocals, field glasses or the telescope"); United States v. Lee, 274 U.S. 559, 563 (1927) (ruling that the U.S. Coast Guard's use of a searchlight to spot a boat at sea "is comparable to the use of a marine glass or a field glass" and "is not prohibited by the Constitution").

147. The Court first formalized this category of cases in *Kyllo v. United States*, in which federal agents suspected the defendant of growing marijuana inside his house; to determine whether this was likely to be true, the agents scanned the defendant's house with a thermal imager, hoping to detect heat signatures typical of the high-intensity lamps used in marijuana cultivation. 533 U.S. 27, 29 (2001). When the imager revealed heat signatures, the agents obtained a search warrant and seized more than 100 marijuana plants from the defendant's residence. Sam Kamin, *The Private Is Public: The Relevance of Private Actors in Defining the Fourth Amendment*, 46 B.C. L. REV. 83, 115 (2004). On appeal, the Court ruled that the use of the imager constituted a search because the defendant had a reasonable expectation of privacy regarding information about the interior of his house that the agents were only able to obtain using technology not in general public use. *See Kyllo*, 533 U.S. at 34 (noting that "obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area' constitutes a search—at least where (as here) the technology in question is not in general public use." (quoting Silverman v. United States, 365 U.S. 505, 512 (1961))).

148. *See* Kamin, *supra* note 147, at 113 (noting that, when the risk of an invasion of privacy "is one that defendants face from their peers, their failure to protect themselves from it is an indication that they do not have a reasonable expectation of privacy").

149. *Id.*

150. *Id.* at 115.

For example, police may use binoculars, cameras with telephoto lenses, or perhaps even remotely operated surveillance cameras[151] to view the subjects of their surveillance at closer range without the subjects' knowledge, provided that such cameras only allow the police to see what they could have otherwise seen unaided, and that there is a public awareness of the technology at issue.[152]

But the intelligence gathering that police forces like those in Los Angeles and New York City are conducting in the wake of September 11 may not even go that far. In many cases, news reports indicate that human intelligence, rather than technology, is the main component of these police departments' efforts,[153] and officers focus on collecting information about daily life simply by being present at cafes, bookstores, mosques, cricket matches, and many other such places[154]—public vantages if ever there were any.

2. Assumption of Risk

Another tactic that police commonly use as part of widespread surveillance and intelligence-gathering operations is to employ informants within the neighborhoods and community groups subject to surveillance.[155] Through the use of such informants, police can gather detailed information about neighborhoods, individuals, and organizations that might otherwise be inaccessible or difficult to target with visual surveillance conducted from public vantage points.[156]

Within the context of widespread surveillance and intelligence gathering, current Fourth Amendment jurisprudence allows police to

151. *See supra* notes 35, 38 and accompanying text.

152. *See supra* note 145 and accompanying text.

153. *See supra* Part II.B.1–2. In fact, some residents of the areas under surveillance may be imagining a greater use of technology than is actually taking place—which leads one to wonder whether these individuals might be inadvertently undermining their own Fourth Amendment protections by expecting less privacy than what they actually enjoy. *See* Kaplan, *supra* note 11, at 44, 46 ("Suspicion of spying is so rife among antiwar activists . . . that some begin meetings by welcoming undercover cops who might be present.").

154. *See* Hawley, *supra* note 89 (noting police spying in on cricket games, in ethnic clubs, in bookstores, and in cafes); Apuzzo et al., *supra* note 101 (noting undercover police investigation at mosques).

155. In New York City, for example, reports indicate that police will often arrest Muslim residents for traffic violations or outstanding warrants and then use the arrests as leverage for convincing those individuals to become police informants. *See* Bennet, *supra* note 85.

156. *See* Harris, *supra* note 80, at 168 (suggesting that the use of informants in Muslim communities enables police to obtain the "maximum possible flow of intelligence on potential terrorist threats").

make broad use of informants "at any point, and for any reason, without judicial supervision."[157] The reason for this is the so-called assumption-of-risk doctrine—occasionally also called the misplaced-confidences doctrine[158]—under which the Courts have found that those who fall victim to police informants generally cannot invoke their Fourth Amendment rights, for both procedural[159] and substantive[160] reasons. And while the idea of assumption of risk may be a "curious way to discuss the use of informants"[161]—more intuitively, informants act as government agents in all but name—the doctrine was firmly established through a series of three Supreme Court decisions handed down in the 1960s and early 1970s: *Lopez v. United States*,[162] *Hoffa v. United States*,[163]

157. *Id.* at 142.

158. Petrashek, *supra* note 122, at 1529.

159. Procedurally, like nearly all constitutional provisions, the Fourth Amendment only limits government conduct, not conduct by private actors, and because any alleged invasion of privacy in this context occurs as a result of the informant's actions, there is no government conduct at issue. *See* Harris, *supra* note 80, at 144 ("Because intelligence gathered by informants is categorized as a result of assumed risk rather than a result of police action, the Fourth Amendment does not regulate the gathering of such evidence.")

160. Substantively, by revealing previously secret information in public (such as by telling it to an informant), individuals must "assume[] the risk that their secrets [will] end up in the possession of the government," and therefore lose any reasonable expectation of privacy they may have had—a key element for claiming Fourth Amendment protections in the post-*Katz* era. Orin S. Kerr, *The Fourth Amendment in Cyberspace: Can Encryption Create a "Reasonable Expectation of Privacy?,"* 33 CONN. L. REV. 503, 511 (2001); *see also supra* notes 134–37 and accompanying text.

161. Harris, *supra* note 80, at 142–43.

162. Lopez v. United States, 373 U.S. 427 (1963). In *Lopez*, an IRS inspector confronted Lopez about nonpayment of taxes on the hotel Lopez owned, whereupon Lopez offered the inspector a bribe to clear the delinquency. *Id.* at 429–30. The inspector reported the bribe to his superiors, and also recorded subsequent conversations with Lopez in which Lopez offered the inspector additional bribes. *Id.* at 430–31. A jury later found Lopez guilty of bribery on this evidence. *Id.* at 434. Lopez argued on appeal that this evidence—the recorded conversations and the inspector's reports to his superiors—was obtained in violation of the Fourth Amendment, *id.* at 437, but the Court noted that the inspector was present by Lopez's consent, and concluded that "the risk [Lopez] took in offering a bribe . . . fairly included the risk that the offer would be accurately reproduced in court." *Id.* at 439.

163. Hoffa v. United States, 385 U.S. 293 (1966). *Hoffa* involved the union boss James Hoffa, who, while on trial for violations of the Taft-Hartley Act, met with various union officials in his hotel room and discussed plans to bribe the jury. *Id.* at 294, 296. Hoffa was unaware that one of these officials, Edward Partin, was relaying Hoffa's conversations to federal agents, who then used this evidence to convict Hoffa of attempted bribery. *Id.* at 296. Although Hoffa acknowledged that he disclosed his bribery plans to Partin willingly, Hoffa argued on appeal that this "consent" should be vitiated because he did not know Partin would later convey his words to the government as an informant. *Id.* at 300. Relying on *Lopez*, the Court responded that it had never "expressed the view that the Fourth Amendment protects

and *United States v. White*.[164]

It is apparent from this line of cases that, although this doctrine is "fairly straightforward," it nevertheless has "serious implications" for the privacy of the targets of police intelligence-gathering operations.[165] Doubtless some of the doctrine's side effects are desirable when it comes to genuinely illegal conspiracies, giving criminals and terrorists alike considerable pause before they consort with one another.[166] But in the case of widespread intelligence-gathering and surveillance efforts, such as those discussed in this Comment, these side effects will spill over onto the vast number of citizens who are *not* engaged in any kind of criminal activities. Because the Court has chosen to focus its Fourth Amendment jurisprudence only on the privacy rights of individuals, and

---

a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it." *Id.* at 302. Somewhat ominously, the Court concluded, "[t]he risk of being . . . betrayed by an informer . . . is probably inherent in the conditions of human society[, and] is the kind of risk we necessarily assume whenever we speak." *Id.* at 303 (quoting *Lopez*, 373 U.S. at 465 (Brennan, J., dissenting)).

164. United States v. White, 401 U.S. 745 (1971). In *White*, the defendant was convicted of engaging in illegal transactions involving narcotics, and much of the evidence against White came from conversations between White and an informant that were relayed to government agents by a radio transmitter concealed on the informant's person. *Id.* at 746–47. Given that the Court had by now held in *Katz* that warrantless wiretaps were an invasion of an individual's privacy, 389 U.S. at 358–59—a decision that had not previously been in place for the defendants in *Lopez* and *Hoffa*—White argued on appeal that, without a warrant, using an informant who was wearing a wire was similarly impermissible. *See White*, 401 U.S. at 749 ("The Court of Appeals understood *Katz* to render inadmissible against White the agents' testimony concerning conversations that [the informant] broadcast to them."). But the Court once again refused to apply the Amendment, reasoning that "[i]f the law gives no protection to the wrongdoer whose trusted accomplice is or becomes a police agent, neither should it protect him when that same agent has recorded or transmitted the conversations which are later offered in evidence to prove the State's case." *Id.* at 752. The Court thus concluded that, like Lopez and Hoffa before him, White had no reasonable (or "constitutionally justifiable") expectation of privacy, and could not shield himself with the Fourth Amendment. *See id.* at 751–53.

165. *See* Petrashek, *supra* note 122, at 1529. The author asserts "serious implications" only with respect to privacy in the context of social networking, *id.*, but given the breadth of the doctrine, its implications are clearly serious for privacy in any context.

166. Justice White eloquently described the doctrine's effect on the economy for criminal conspirators in *United States v. White* when he wrote,

> Inescapably, one contemplating illegal activities must realize and risk that his companions may be reporting to the police. If he sufficiently doubts their trustworthiness, the association will very probably end or never materialize. But if he has no doubts, or allays them, or risks what doubt he has, the risk is his.

United States v. White, 401 U.S. at 752.

not the shared privacy of groups,[167] and because the police have almost unlimited license to use informants, this broader result can hardly be called desirable. As the size of a person's social network increases, so too does the risk that an acquaintance may be a police informant, forcing individuals to be unnecessarily selective in the acquaintances they make[168]—and leaving them with no recourse against the government in the event that even this level of heightened suspicion turns out to be misguided.

3. Third Parties

In addition to the police tactics discussed in the previous two sections (visual surveillance and the use of informants), a hallmark of the intelligence operations being established within local law enforcement agencies post-September 11 is a strong focus on data-mining—gathering vast amounts of data from which police analysts might discern behavioral patterns and cultural norms that help to identify and prevent the next terrorist attack.[169] The information in police databases could potentially come from not only surveillance reports and informants, but also from independent third parties, such as telephone companies, banks, and even the U.S. Census Bureau.[170] Although several commentators have argued that data-mining has yet to prove itself a viable tool in law enforcement's counterterrorism toolkit,[171] it remains a fixture of intelligence efforts.[172]

---

167. Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1136–37 (2002).

168. *See* Petrashek, *supra* note 122, at 1529–30 (noting that the only way a person may protect himself from informants is to select his friends with care, and that "there is a direct relationship between the number of recipients [of information] and the risk that one or more of them will use the information . . . in a way harmful to the communicator").

169. *See* MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY 316 (11th ed. 2011) (defining data-mining as: "the practice of searching through large amounts of computerized data to find useful patterns or trends"); Katherine J. Strandburg, *Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance*, 49 B.C. L. REV. 741, 746 (noting that data mining "was given a huge boost after September 11, 2001, when [law enforcement's] attention focused on tracking terrorist networks").

170. *See* Apuzzo & Goldman, *NYPD Spies*, *supra* note 79 (documenting NYPD's usage of surveillance reports and informants); Winton, *Outcry*, *supra* note 50 (explaining the LAPD's use of U.S. Census bureau information to plan its mapping project); *infra* note 180 (explaining the Court's holding in *Miller* that banks can give out people's records, as they have no right of privacy in those records); *infra* note 182 (explaining Court's holding in *Smith* that a person has no right of privacy over their phone records held by their telephone companies).

171. Daniel J. Solove, *Data Mining and the Security-Liberty Debate*, 75 U. CHI. L. REV.

Most of this information is not subject to Fourth Amendment protections because of the third-party doctrine, which holds that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[173] A cousin of the assumption-of-risk doctrine—both count *Hoffa* among their ancestors[174]—the third-party doctrine is one of the most criticized exceptions to the Fourth Amendment's scope, and there have been numerous calls to overhaul or eliminate it.[175] But much like the data-mining it permits, the doctrine appears to be here to stay. The Court has refused to find that many common data-mining practices implicate constitutionally protected privacy rights; instead, the Court has left the work of creating boundaries to Congress, which has done so selectively and not always successfully.[176]

The doctrine got its start in *Katz*, where the Court issued its now-famous statement that "[w]hat a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection,"[177] and the Court also hinted at the doctrine in *Hoffa*,[178] *Couch v. United States*,[179] and *United States v. Miller*.[180] But the doctrine truly ripened in *Smith v.*

343, 362 (2008) [hereinafter *Data Mining*].

172. *See id*. at 353. This is partly because of successful marketing campaigns by database companies, *id.*, but also because past experience has shown that, at least in theory, data-mining could prevent terrorist attacks. *See* BJELOPERA, *supra* note 77.

173. *E.g.*, Smith v. Maryland, 442 U.S. 735, 743–44 (1979); *see* Petrashek, *supra* note 122, at 1518–19 (discussing the implications of the *Smith* decision).

174. *See* Lalli, *supra* note 141, at 259 (noting that the Court relied on the third-party doctrine in *Hoffa*).

175. *See, e.g.*, Jim Harper, *Reforming Fourth Amendment Privacy Doctrine*, 57 AM. U. L. REV. 1381, 1382 (2008) (calling *Smith* "regrettable"); Lalli, *supra* note 141, at 261–64 (summarizing three different critiques of the third-party doctrine, the common theme of which is that the doctrine is "outdated").

176. *See infra* Part IV.A.

177. Katz v. United States, 389 U.S. 347, 351 (1967).

178. Though the Court in *Hoffa* conducted its analysis primarily using the language of risk, it emphasized that Hoffa took no measures to conceal his conversations from third parties. *See* Hoffa v. United States, 385 U.S. 293, 302 (1966) (noting that "every conversation [the informant] heard was either directed to him or knowingly carried on in his presence").

179. Couch v. United States, 409 U.S. 322, 335–336 (1973); *see* David S. Barnhill, Note, *Cloud Computing and Stored Communications: Another Look at* Quon v. Arch Wireless, 25 BERKELEY TECH. L.J. 621, 627-28 (2010) (describing the Court's holding in *Couch* that a woman's reasonable expectation of privacy in her tax records "vanished" once she gave them to an accountant).

180. United States v. Miller, 425 U.S. 435, 441–443 (1976); *see* Lalli, *supra* note 141, at 260 (describing the Court's holding in *Miller* that a bank customer "had no protectable Fourth Amendment privacy interest in his bank records because they were held by third

Maryland,[181] such that a party now essentially relinquishes his privacy interest in a piece of information at the same time he relinquishes the information itself.[182]

The third-party doctrine has held up in subsequent court decisions,[183] and it has become particularly worrisome to civil liberties advocates in a digital era in which individuals transmit large amounts of data and information across the Internet.[184] By uploading files to Internet services like Facebook, Twitter, Craigslist, Google, and others, individuals transfer that information to third parties and, in theory, relinquish their Fourth Amendment-protected privacy interests in the information.

While in principle the question of whether individuals relinquish their Fourth Amendment protections under these circumstances is an open question,[185] in practice it may be a different matter. Some have noted that, in *Smith*, the Court took pains to establish a "content/envelope distinction"—when transferring information to a third party, a person loses their privacy interest only in the "envelope" (the part of the information used by the third party for handling purposes, such as the telephone digits in *Smith*) and not in the content (the "hidden" part of the message, such as the actual, audible telephone

---

parties").

181. Smith v. Maryland, 442 U.S. 735 (1979). In *Smith*, the victim of a robbery reported "receiving threatening and obscene phone calls from a man identifying himself as the robber." *Id.* at 737. Police used information from the victim to identify Smith as the suspect, and then, without a warrant, asked the telephone company to install a pen register to record the numbers dialed on the telephone at Smith's house. *Id.* When Smith once again called the victim, police were able to match the numbers dialed by Smith to the call received by the victim, evidence that eventually led to Smith's conviction. *Id.* at 737–38. Smith sought to suppress the pen register as an unconstitutional search under the Fourth Amendment, *id.* at 737, but on appeal the Court said that Smith had no legitimate expectation of privacy with respect to the numbers he dialed on his phone. *Id.* at 742. Given that most telephone users realize they must "convey" the numbers they dial to a telephone company in order to place a call, the Court concluded it was "too much to believe that telephone subscribers . . . harbor any general expectation that the numbers they dial will remain secret." *Id.* at 742–43.

182. *See id.* at 743–45.

183. *See, e.g.*, United States v. Scott, 975 F.2d 927, 929 (1st Cir. 1992) (holding that "a person who places trash at a curb to be disposed of or destroyed by a third person [renounces] . . . 'any reasonable expectation of privacy in the property abandoned'" (quoting United States v. Mustone, 469 F.2d 970, 972 (1st Cir. 1972))).

184. *See* Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 B.C. L. REV. 1511, 1531 (2010) (noting that files uploaded to third-party Internet sites could fall outside of the Fourth Amendment's protections) [hereinafter *Fourth Amendment Pragmatism*].

185. The Supreme Court has not yet decided "whether and how the third-party doctrine applies to Internet communications." Petrashek, *supra* note 122, at 1520.

conversation in *Smith*).[186] Like telephone calls, Internet communications have envelope and content components, suggesting that a consistent application of the third-party doctrine would recognize at least some Fourth Amendment protections in messages being sent and documents being uploaded. But many other scholars have noted the sheer breadth of the third-party doctrine,[187] which in addition to offering little hope for defendants, also makes it difficult for commentators to predict how (or even whether) the Court will adapt it to meet the realities of the Internet-era docket.[188]

Indeed, many of those same scholars have predicted the Court will continue to apply the doctrine "to all personal information possessed by third parties,"[189] and they do not appear to be wrong. The Court has made no moves to reverse course in this area, and in the current political climate, "[t]he scale is rigged so that security will win out [over civil liberties] nearly all the time."[190] As a result, at least from a Fourth Amendment standpoint, there is no restriction on the police's ability to gather large amounts of data that individuals have disclosed to third parties. The third-party doctrine may be a gold mine for police in their efforts to establish widespread intelligence networks, but the constant transfer of information that characterizes modern society means that the doctrine also exposes vast numbers of Americans to potential privacy invasions while giving them little realistic opportunity to call the government to account.

IV. THE NEXT-BEST THING—PRIVACY FROM WIDESPREAD POLICE SURVEILLANCE AND INTELLIGENCE GATHERING BEYOND THE FOURTH AMENDMENT

Though the Fourth Amendment may offer individuals little protection against the investigative practices of police intelligence units, there are still other ways that individuals might preserve their privacy.

186. *See* Achal Oza, Note, *Amend the ECPA: Fourth Amendment Protection Erodes as E-Mails Get Dusty*, 88 B.U. L. REV. 1043, 1049 (2008) (analyzing the envelope/content distinction with respect to telephone calls and postal mail).

187. *See* Richard A. Epstein, *Privacy and the Third Hand: Lessons from the Common Law of Reasonable Expectations*, 24 BERKELEY TECH. L.J. 1199, 1200 (2009).

188. *See, e.g.*, *Fourth Amendment Pragmatism*, *supra* note 184, at 1531–32 (noting the debate of whether and how the third-party doctrine applies to Internet cases is "difficult to resolve because the Supreme Court's decisions are incoherent").

189. *Id.* at 1531.

190. *Data Mining*, *supra* note 171, at 362.

This Part discusses what might be considered the best alternative to constitutional protections—statutory restrictions on police surveillance and intelligence gathering. This Part first seeks to explain why statutes are a legitimate alternative to constitutional protections, and then discusses the competing interests—individual privacy and national security—that must be addressed in any potential statute limiting police conduct in this area.

A. Legislative Definitions of Privacy Augment Constitutional Definitions

As the previous Part illustrates, today's constitutional notions of privacy and the Fourth Amendment's protections of those notions are relatively narrow in scope,[191] having receded from the high point of *Katz* thanks to the variety of exceptions that the Court has carved out in the intervening years. Fortunately for individuals who may be subject to police surveillance, privacy law in the United States is "vast and complex," and includes not only the Fourth Amendment, but "dozens of federal privacy statutes, and hundreds of state privacy statutes."[192]

It is true the Fourth Amendment is unquestionably the most important of these laws, the cornerstone of privacy in America. But it is also, to continue the metaphor, the foundation of privacy in America, laid by the courts as a starting point upon which additional limitations and regulations may be built.[193] History supports this idea. After the Supreme Court decided in *Olmstead* in 1928 that wiretapping was not subject to the Fourth Amendment's protections,[194] Congress soon moved to fill the gap, passing the Communications Act of 1934, which placed significant restrictions on wiretapping.[195] When the Court later decided

191. *See* Omer Tene, *What Google Knows: Privacy and Internet Search Engines*, 2008 UTAH L. REV. 1433, 1474 (2008) (describing constitutional privacy protection as narrow in the United States, especially when compared to equivalent protections in Europe).

192. Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 483 (2006) [hereinafter *Taxonomy of Privacy*]; *see also* Katie Stenman, *State Government Information Collection: The Shutdown of the MATRIX Program, REAL ID, and DNA Collection*, 2 I/S: J.L. & POL'Y INFO. SOC. 547, 548 (2006) ("Ten state constitutions explicitly recognize a right to privacy, and many states have additional laws protecting various types of privacy. . . . State laws protect these different types of privacy to varying degrees.").

193. *See* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 858 (2004) (noting that "courts have successfully created rules that establish important privacy rights in many areas").

194. *See supra* notes 116–20.

195. Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581,

that wiretaps *did* fall under the Fourth Amendment in *Katz*,[196] Congress augmented this position with additional rules in Title III of the Omnibus Crime Control and Safe Streets Act of 1968.[197]

More recently, in the 1970s and 1980s, Congress passed a number of other laws establishing privacy protections beyond those offered by the Court in its Fourth Amendment jurisprudence, many of them in response to decisions handed down by the Court.[198] The most noteworthy law to come out of this period is the Electronic Communications Privacy Act of 1986, which was originally enacted to protect Americans' privacy interests in their e-mail,[199] but has since been amended to bring other forms of technological information under its umbrella as well.[200] In contrast to the Court's reluctance to develop specific privacy protections under the Fourth Amendment, Congress and the state legislatures have been quite active in this area.

Despite this activity, the resulting statutes provide what is best described as a patchwork of protection of individuals' privacy interests. There is no general privacy law in the United States,[201] only laws that guard certain privacy interests in certain types of information or contexts.[202] One possible rationale behind this scheme is that, in most cases, when individuals relinquish private information about themselves, they do so in a contract-like exchange in which they are able to negotiate the terms and assess whether the loss of privacy is worth the

591–92 (2011). Despite the noble intentions behind the Communications Act, however, it appears the Act was less than successful in achieving its desired end, as the FBI was able to continue its widespread use of wiretaps even after the Act was passed. *Id.* at 592.

196. *See supra* notes 106, 109.

197. *See Taxonomy of Privacy*, *supra* note 192, at 492–93 (summarizing Title III's requirement that "law enforcement officials [must] obtain a warrant before wiretapping," and its prohibition on the private use of wiretaps).

198. *See* Kerr, *supra* note 193, at 855–56 (summarizing a number of privacy laws passed by Congress during this period).

199. *Id.* at 856 ("Congress protected the privacy of stored e-mails and Internet communications by passing the Electronic Communications Privacy Act.").

200. *Id.* at 871. The law has been amended eleven times since 1986, although some of these amendments were admittedly "minor technical amendments." *Id.*

201. *See* Daniel E. Newman, *European Union and United States Personal Information Privacy, and Human Rights Philosophy—Is There a Match?*, 22 TEMP. INT'L & COMP. L.J. 307, 338 (2008).

202. *Id*. (noting several, including: the Health Insurance Portability and Accountability Act of 1996 (HIPAA) for medical records; the Graham-Leach-Bliley Act of 1999 (GLBA) for financial records; and the Children's Online Privacy Protection Act of 1998 (COPPA), for information collected from children on the Internet).

consideration they will receive in return;[203] privacy legislation exists only to level the playing field in those situations where individuals lack the ability to negotiate.[204] The other reason why this scheme may exist is that Congress prefers to legislate only when necessary, waiting until the Court has defined a particular contour of the Fourth Amendment.[205] But this is a less-than-ideal approach, because, like most constitutional provisions, the Amendment is better used as a tool for evaluating statutes than for prescribing rules to fill the void.[206] Whatever the reasons behind this scheme, the point remains: Existing statutory protections of privacy—though they provide broader coverage than the Fourth Amendment—still leave unregulated many of the police surveillance and intelligence-gathering tactics discussed in this Comment.

That does not mean, however, we should abandon the legislature as a hope for better privacy protections, resigning ourselves to exploring the nooks and crannies of Fourth Amendment case law in search of some way of preserving individuals' privacy against widespread police surveillance. Far from it. Although a number of scholars believe the judiciary is in the best position to guide privacy doctrine,[207] Professor Orin Kerr[208] has made a convincing case that the legislative approach is

203. *See id.* at 336–38 (suggesting that federal personal-privacy law is based on contract law and discussing the process of bargaining away personal data in the private market).

204. *See id.* at 336–37 (noting that the statutory framework for privacy in the United States "appears to be predicated on ideas from contract law" but that "Congress was willing to enact privacy legislation for the government, because people often lack a meaningful choice when dealing with the government"). For example, it is well understood that if an individual buys a product over the Internet, she must relinquish private information about herself—name, address, credit card number—to obtain the product. The possibility that the vendor will expose this information to the public is low, and is offset by the convenience of online shopping. If the Internet vendor does mishandle her information, then she can easily choose not to do business with that vendor in the future. But the same individual has no ability to negotiate with the government, or take her "business" elsewhere if the government uses her information for ends to which she did not consent.

205. *See* Tokson, *supra* note 195, at 596 (noting that in the past, Congress has waited "for the Supreme Court to clearly define the scope of Fourth Amendment protection for new technologies before taking any legislative action").

206. *See Fourth Amendment Pragmatism*, *supra* note 184, at 1529.

207. *See, e.g.*, Tokson, *supra* note 195, at 596 (asserting that most scholarship on the Fourth Amendment's third-party doctrine takes as a given the courts' role as arbiters in "determining reasonable expectations of privacy in new technologies").

208. Professor Orin Kerr teaches criminal law and criminal procedure at George Washington University, where he has been a member of the faculty since 2001. *GW Law Faculty Directory: Orin S. Kerr*, GEO. WASH. LAW SCH., http://www.law.gwu.edu/Faculty/pro

better because legislatures are not limited by the three significant constraints courts face on a regular basis.

First, courts create rules "ex post in a case-by-case fashion," meaning that courts cannot apply the Fourth Amendment to new developments in police tactics until cases involving those tactics come before them—assuming the cases arise at all.[209] In contrast, "[l]egislatures can act at any time," even anticipating emerging investigative methods and proscribing or limiting them in advance.[210] Second, by the principle of stare decisis, courts are bound to follow prior decisions, even if outdated.[211] Though it has the benefit of making judicial decisions more predictable, stare decisis also gives the courts less flexibility; legislatures, on the other hand, can take a more dynamic approach, designing laws to meet the evolving needs of society.[212] Finally, courts can generally only consider the facts of a given case, but legislatures can act upon a "wide range of inputs, ranging from legislative hearings and poll results to interest group advocacy," resulting in more informed legislation.[213] Given these factors, legislation seems more likely to offer better protections and the possibility of redress to the subjects of unwarranted police surveillance than any attempt to challenge the practices under the Fourth Amendment.

B. Any Legislation that Protects Individuals from Police Surveillance Must Sufficiently Address the Interests at Stake

Any legislation limiting police intelligence-gathering and

file.aspx?id=3568 (last visited Sep. 16, 2012) (click on curriculum vitae link for a list of classes taught). The author of several criminal law casebooks, he has been cited in at least one decision by every regional United States Court of Appeals and by one account is the seventh-most cited criminal law scholar. *Id.*

209. Kerr, *supra* note 193, at 868–69 (detailing the numerous procedural obstacles that a constitutionally questionable police tactic must overcome before a court may decide its legality—even at the lowest levels of our judicial system).

210. *Id.* at 870.

211. *See* Richard J. Dougherty, *Originalism and Precedent: Principles and Practices in the Application of Stare Decisis,* 6 AVE MARIA L. REV. 155, 157–58 (2007).

212. Kerr, *supra* note 193, at 871; *see also* Tokson, *supra* note 195, at 595–96 (arguing that the "potential error costs of legislation may be lower than those of constitutional decision making. Flawed statutes are relatively easy to amend, while erroneous Fourth Amendment decisions could require a constitutional amendment to overturn").

213. Kerr, *supra* note 193, at 875. For an argument that the judiciary holds some advantages over the legislature, see *id.* at 882 (acknowledging that the judiciary's independence can sometimes be an asset, especially when legislation is the product of disproportionately well-funded special-interest groups).

surveillance activities must sufficiently take into account the two competing sets of interests driving the debate—individuals' privacy interests and society's collective interest in national security. These interests are intensely held by wide swaths of the public, and, for many individuals, these interests' importance vis-à-vis each other are likely to change over time in response to current events. The purpose of this section is to define these interests more clearly, in the belief that any legislation that does not take these interests into account will be ineffective or, worse, unlikely to pass at all.

1. Privacy

The general consensus among privacy scholars is that privacy is, as Hemingway might have put it, a fine thing and worth fighting for.[214] Most discussions of the concept begin by asserting, for example, that privacy is a "self-evident good"[215] consistent with the "aims of a free and open society."[216] A number of these discussions have identified protected privacy rights throughout history,[217] while others rely on the thorough discussions of privacy rights as natural rights conducted by the great philosophers of the Enlightenment.[218] But so often these tributes to the greatness of privacy fail to consider why—or even whether—privacy is something worth protecting with the force of law. Even *The Right to Privacy*,[219] the famous 1890 *Harvard Law Review* article by Samuel Warren and Louis Brandeis—widely regarded as the first piece of American legal scholarship to advocate for a right to privacy in a civil

214. *See* ERNEST HEMINGWAY, FOR WHOM THE BELL TOLLS 502 (1940) ("The world is a fine place and worth the fighting for and I hate very much to leave it.").

215. David Rosen & Aaron Santesso, *Inviolate Personality and the Literary Roots of the Right to Privacy*, 23 L. & LITERATURE 1, 2 (2011).

216. United States v. Hendrickson, 940 F.2d 320, 322 (8th Cir. 1991) (quoting WAYNE R. LAFAVE & JEROLD H. ISRAEL, 1 CRIMINAL PROCEDURE 165 (1984)).

217. *See, e.g.*, Jeremy Osborne, *Ascending the Slippery Slope: New Alabama Law Enforcement Procedures Fail to Adequately Protect Sexual Assault Victims' Privacy*, 5 GEO. J.L. & PUB. POL'Y 785, 787–88 (2007) (identifying privacy rights in the Hebrew Torah and in ancient Greece).

218. *See, e.g.*, Henry F. Fradella et al., *Quantifying* Katz*: Empirically Measuring "Reasonable Expectations of Privacy" in the Fourth Amendment Context*, 38 AM. J. CRIM. L. 289, 320 (2011) (discussing the beliefs of the seventeenth-century-English philosopher John Locke, who argued that individual autonomy and private property were inalienable natural rights). In drafting the Declaration of Independence and the Constitution, the Founding Fathers drew heavily on Enlightenment philosophers. *Id.* at 321.

219. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890) (recommending the creation of a new tort to protect individual privacy).

law context—has since been criticized as too vague in describing its conception of privacy.[220]

The result is that the notion of "privacy" has come to be a powerful but oftentimes meaningless incantation, invoked reflexively in a wide array of contexts without much more than lip service as to its actual importance.[221] Although privacy may have longstanding traditions in both history and natural law, such justifications can appear especially bland or ill-defined when stacked against more timely and more concrete interests like national security.[222] In light of this, it is worth discussing why individuals' privacy interests are worth protecting in the face of police intelligence-gathering activities—such as widespread visual surveillance, the use of informants, and data-mining—all of which significantly reduce the amount of privacy available to individuals as a practical matter.

Scholars have identified two main effects that a reduction in privacy will have on individuals and, in the aggregate, on society as a whole. The first category contains psychological effects, which have been thoroughly studied by experts. "Failure to be able to achieve privacy," such as would occur under conditions of near-constant surveillance, can have "devastating psychological effects, such as deindividualization and dehumanization."[223] At a basic level, individuals subject to such surveillance will begin to lose the "freedom of thought and mind."[224] In more extreme cases antisocial behavior will likely result.[225] One well-documented example of this—which also provides a better glimpse at the concept of total surveillance than we might like to admit—occurs

220. *See* Rosen & Santesso, *supra* note 215, at 4–6 (summarizing the various criticisms of *The Right to Privacy*, and asserting that "even critics sympathetic to the conclusions Warren and Brandeis offer . . . have experienced difficulties perceiving the paper's reasoning").

221. *See Taxonomy of Privacy*, *supra* note 192, at 479–80 (noting that "'[p]rivacy is a chameleon-like word," used in "knee-jerk" fashion to "appeal to people's fears and anxieties" (quoting Lillian R. BeVier, *Information About Individuals in the Hands of Government: Some Reflections on Mechanisms for Privacy Protection*, 4 WM. & MARY BILL RTS. J. 455, 458 (1995))).

222. *See id.* at 480 (discussing the imbalance between vague discussions of privacy interests and opposing interests that are "much more readily articulated").

223. Fradella et al., *supra* note 218, at 304.

224. *See* Anuj C. Desai, *Can the President Read Your Mail? A Legal Analysis*, 59 CATH. U. L. REV. 315, 344 (2010) (arguing that certain privacy protections further the values of "freedom of thought and mind").

225. Fradella et al., *supra* note 218, at 304 (citing Darhl M. Pedersen, *Psychological Functions of Privacy*, 17 J. ENVTL. PSYCHOL. 147, 147 (1997)).

with Hollywood celebrities, who sometimes suffer emotional breakdowns because they cannot escape the paparazzi.[226] Based on the descriptions of police intelligence-gathering operations reported in the media, it does not take a significant conceptual leap to imagine that those subject to such surveillance might quickly come to feel the same intense lack of privacy and the "extremely uncomfortable" psychological effects that go with it.[227]

The second category of side effects caused by a lack of privacy includes behavioral effects, which can have a wide range of implications. When individuals become aware of near-constant surveillance, they begin to self-censor their normal behavioral patterns.[228] This, in turn, enhances "the power of social norms," as most self-censorship will involve individuals seeking to conform to mainstream societal boundaries.[229] The result is a chilling effect on "eccentric individuality," not only in fact, but also in our innate desire to realize such individuality.[230] While under some circumstances this might be considered a positive aspect of certain narrowly defined police activities that deprive individuals of their privacy,[231] intelligence-gathering programs like those described here are hardly "narrowly defined," and are much more likely to affect individuals who have only a tenuous connection to the target of the surveillance.

Some will argue that secret police intelligence gathering will not have these effects, or at the very least, its effects will be minimized because much of this surveillance is secret and the targets are unaware of its existence. This is not likely true. Police intelligence programs have, by now, been widely reported in the news media,[232] and once the public has gained a general awareness of the possibility of surveillance through such programs, the mere fact of its existence can exert the same

226. *Id.* It is worth noting that lack of privacy can occur not only through surveillance but also through the "public disclosure of highly personal information." *Id.*

227. *Taxonomy of Privacy*, *supra* note 192, at 493.

228. *Id.*

229. *See id.* (noting that "surveillance is a tool of social control, enhancing the power of social norms, which work more effectively when people are being observed by others in the community").

230. *Id.* at 494 (quoting Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1426 (2000)).

231. *See id.* (acknowledging that surveillance can be a valuable social control when it comes to deterring crime).

232. *See supra* Part II.B.

psychological and behavioral effects on individuals.[233]

Enacting legislation that effectively limits police intelligence gathering and protects individuals' privacy interests thus has several important functions. First, it would restore the public's psychological confidence in its own privacy, assuring individuals that they need not fear imagined possibilities in a constant state of paranoia. Second, it would provide significant societal benefits, limiting the possibility for antisocial behavior that comes with reduced privacy. Finally, it would eliminate or reduce the need for self-censorship, at least in certain circumstances, encouraging the diversity of thought, opinion, and behavior that is characteristic of liberal democracies. All noble goals—but this is only half the story. This Part next considers the opposing interest, national security.

2. National Security

As with privacy, assessing the importance of national security as an interest to be protected is not a standalone inquiry; defending the country from terrorist attacks and other foreign threats is a legitimate and important purpose of the state.[234] The inquiry here is why and when such an interest should be elevated above constitutionally protected civil liberties like privacy. It is critical such circumstances are taken into account with respect to any proposed legislation that would limit police surveillance and intelligence-gathering practices, because "no governmental interest is more compelling than the security of the Nation."[235] The government must be able to provide this security when

---

233. Professor Daniel Solove of George Washington University Law School discusses this concept within the context of the Panopticon, a theoretical prison designed by the eighteenth-and nineteenth-century philosopher Jeremy Bentham:

> The prison was set up with the inmates' cells arrayed around a central observation tower. Most importantly, the guards could see each prisoner from the tower, but the prisoners could not see the guards from their cells. . . . The prisoner's "only rational option" was to conform with the prison's rules because, at any moment, it was possible that they were being watched. Thus, awareness of the possibility of surveillance can be just as inhibitory as actual surveillance.

Taxonomy of Privacy, *supra* note 192, at 495 (footnotes omitted) (citing DAVID LYON, THE ELECTRONIC EYE: THE RISE OF SURVEILLANCE SOCIETY 62–67 (1994)).

234. David S. Eggert, Note, *Executive Order 12,333: An Assessment of the Validity of Warrantless National Security Searches*, 1983 DUKE L.J. 611, 631 (1983).

235. Haig v. Agee, 453 U.S. 280, 307 (1981), *quoted in* Frederic Block, *Civil Liberties During National Emergencies: The Interactions Between the Three Branches of Government in Coping with Past and Current Threats to the Nation's Security*, 29 N.Y.U. REV. L. & SOC.

we need it the most.

As a matter of importance, national security has a long history; by some accounts, American national security predates even America itself.[236] The challenge of preserving that security through more than 235 years of wars, emergencies, economic shocks, and other exigent circumstances, both real and imagined, has produced a number of episodes in which the country has put its security before its civil liberties. In 1798, Congress passed the Alien Act, which gave the President the authority to summarily order the removal of foreign nationals,[237] and the Sedition Act, which prohibited the publication of materials criticizing the government;[238] both laws were passed in response to rising diplomatic tensions with France that had potential implications on domestic politics.[239] President Abraham Lincoln famously suspended habeas corpus rights during the Civil War.[240] During World War I, Congress passed the Espionage Act, which criminalized the "mak[ing] or convey[ance] . . . [of] false statements with intent to interfere with the success of the military . . . when the United States is at war,"[241] and during World War II, President Franklin Roosevelt authorized the internment of Japanese-Americans living on the West Coast.[242] Based on this long history, it took no great amount of prescience for Justice Sandra Day O'Connor to assert, at a speech in New York City less than three weeks after the September 11, 2001 terrorist attacks, that Americans were now "likely to experience more restrictions on personal freedom than has ever been the case in our country."[243] Indeed, civil liberties have once again come under fire in

---

CHANGE 459, 459 (2005).

236. William C. Banks & M.E. Bowman, *Executive Authority for National Security Surveillance*, 50 AM. U. L. REV. 1, 10 (2000) (tracing the origins of national security law to the Committee for Secret Correspondence, which was created by the Continental Congress in 1775).

237. An Act Concerning Aliens, ch. 58, 1 Stat. 570, 571 (1798).

238. Sedition Act, ch. 74, 1 Stat. 596, 597 (1798).

239. Banks & Bowman, *supra* note 236, at 16–17 & n.101 (discussing the circumstances leading to the passage of the Alien and Sedition Acts).

240. *Id.* at 17. The suspension of these rights led to the military detention of more than 20,000 individuals suspected of "disloyalty." Block, *supra* note 235, at 482–83.

241. Espionage Act of 1917, 65 Pub. L. 24, ch. 30, 40 Stat. 217, 219 (1917) (codified as amended at chapter 37, 18 U.S.C. (2000)); *see* Block, *supra* note 235, at 483.

242. *See* Robert N. Davis, *Striking the Balance: National Security vs. Civil Liberties*, 29 BROOK. J. INT'L L. 175, 178 (2003).

243. Justice Sandra Day O'Connor, Supreme Court of the United States, Address at the New York University School of Law Groundbreaking Ceremony (Sept. 28, 2001), *quoted in*

the years following the attacks.[244]

Historically, there have been at least four different arguments used to justify elevating national security above civil liberties, and understanding these reasons is critical for evaluating the relative importance of the interest as a whole. The first argument is that terrorists care little for our civil liberties;[245] as a result, neither should we, because doing so would put us at a dangerous competitive disadvantage.[246] A closely considered formulation of this argument is that our margin for error when dealing with our enemies—especially terrorists—is so small, or even nonexistent, that we need to be able to act without worrying about civil liberties protections.[247] One's response to this argument is likely colored by policy preferences—How much should we be willing to bend the rules in response to an extremist threat?—but giving up on civil liberties entirely seems somewhat defeatist. Ample scholarship, as well as common sense, suggests that a balance can be struck that preserves individual liberties and privacy while allowing us to counter serious threats to our security.[248]

The second argument, which has come into vogue in the late twentieth and early twenty-first centuries, is that our conflicts now

---

Block, *supra* note 235, at 459.

244. *See, e.g.*, Richard Schmitt, *Covert Searches Are Increasing Under Patriot Act*, L.A. TIMES, May 2, 2004, at A29 (describing civil liberties advocates' concerns over the number of "secret searches" conducted by the Justice Department in the years following the September 11, 2001 terrorist attacks).

245. *See* Michael Goldsmith, *The Supreme Court and Title III: Rewriting the Law of Electronic Surveillance*, 74 J. CRIM. L. & CRIMINOLOGY 1, 34 (1983) (noting that the need for police to "respond in kind" to their enemies "has long been a traditional justification" for making greater use of technology in surveillance).

246. *See* Lisa M. Kaas, Note, *Liberty v. Safety: Internet Privacy After September 11*, 1 GEO. J.L. & PUB. POL'Y 175, 175, 188 (2002) (recalling that Congress passed the USA PATRIOT Act in response to law enforcement's pleas that they needed to be "equipped with the most up-to-date tools in order to combat an increasingly high-tech enemy"); *see also* Goldsmith, *supra* note 245.

247. *See* Eggert, *supra* note 234, at 634 (noting that the Justice Department has argued that "foreign affairs often require prompt and decisive action"); *see also* John Mintz & Michael Grunwald, *FBI Terror Probes Focus on U.S. Muslims*, WASH. POST, Oct. 31, 1998, at A1, A8 (quoting a frustrated senior FBI official as saying, "We know that whenever we do something, people are going to call us jackbooted thugs. But if we do nothing, people are going to yell at us when something blows up"), *quoted in* Ronald J. Sievert, *Meeting the Twenty-First Century Terrorist Threat Within the Scope of Twentieth Century Constitutional Law*, 37 HOUS. L. REV. 1421, 1424 (2000).

248. *See, e.g.*, Davis, *supra* note 242, at 177–78 (arguing that "it is possible for national security legislation to protect civil liberties, while achieving national security objectives," and that national security and civil liberties are "not mutually exclusive").

involve stateless enemies for which there is no effective military response;[249] thus, curtailing civil liberties in certain limited circumstances may be the best or only alternative.[250] The operative word in this argument is "limited." Americans may be willing to recognize limited curtailment of civil liberties in times of emergency, or may be more willing to do so if the curtailment is well-defined.[251] Prospective legislation must take this into account.

The third argument is that national security is a precondition of civil liberties.[252] In other words, civil liberties cannot exist without the nation, and if the nation is threatened, then we must turn our resources toward first protecting the nation; only once the nation is secure can we again worry about the freedoms that we hold dear.[253] Although there is an attractive simplicity to this argument, it is important to note that it hinges on the assumption that the nation faces a dire threat to its existence. Few Americans are in a position to accurately assess such an assumption, which means that, if the government is authorized to take national security measures that endanger civil liberties, the chance of effective oversight may be slight. Any potential legislation must also address this.

The final argument in favor of elevating national security concerns above civil liberties is a procedural one—that there is precedent to support it. In 1978, Congress passed the Foreign Intelligence

249. *See* Sievert, *supra* note 247, at 1427

250. *See id.* at 1427–28 (identifying the "many practical problems associated with the use of military force" against terrorists, such as that they have no easily identifiable "home base" and that their foreign hosts may not be aware of their presence); John C. Yoo, *Judicial Review and the War on Terrorism*, 72 GEO. WASH. L. REV. 427, 429 (2003) (noting that the war on terror is "unconventional" and the enemy "does not seek to defend or acquire any specific territory," compelling the U.S. government to "undertake a full spectrum of domestic and international responses").

251. *See* Emanuel Gross, *How to Justify an Emergency Regime and Preserve Civil Liberties in Times of Terrorism*, 5 S.C. J. INT'L L. & BUS. 1, 22 (2008) (explaining that in the face of terrorism related states of emergency, "the public might urge the government to change the traditional array of constitutional balances between civil liberties and national security in favor of the latter").

252. *See* Davis, *supra* note 242, at 238.

253. *See id.* (asserting that "it becomes very difficult to preserve civil liberties if the survival of the nation is in the balance" and that "by preserving the nation we are better able to preserve freedom"); Kaas, *supra* note 246, at 189 (noting that "the liberties held so dear by so many Americans are made possible in the first place by a government that protects and defends its people against the acts of oppressive regimes").

Surveillance Act (FISA),[254] which generally provides the federal government with the ability to conduct electronic surveillance without a warrant as long as the Attorney General certifies to a special Foreign Intelligence Surveillance Court that there is no "substantial likelihood" that U.S. persons will be a party to the surveillance.[255] Despite that FISA "has been criticized for lacking 'due process and accountability,'"[256] and that its quasi-constitutional structure is not entirely compatible with the Fourth Amendment,[257] the law has "withstood substantial judicial scrutiny"—apparent evidence that, when it comes to intelligence gathering, civil liberties should take a back seat to national security.[258]

But the type of surveillance with which FISA is concerned is an inexact parallel to current police intelligence activities for two reasons. First, and most importantly, the law's scope is limited to foreign nationals; if nothing else, Congress sought to avoid compromising Americans' civil liberties in passing the law. Second, FISA provides a complex set of controls to guard against abuses of surveillance: for example, surveillance applications submitted to the FISA court must be particular in describing the target of the surveillance, and must also describe "minimization procedures" that have been put in place to ensure that Americans do not become subject to such surveillance.[259] It is hardly accurate to characterize FISA as a wholesale suspension of civil liberties, especially with respect to Americans, and it is equally inaccurate to claim that there is legal precedent that supports unlimited police surveillance. Nevertheless, like the other arguments discussed here, its presence in the scholarship illustrates just how compelling an interest national security is—and one that must be considered in drafting any legislation that would limit police surveillance.

---

254. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 110-261, 112 Stat. 2436 (codified as amended in scattered sections of 50 U.S.C.).

255. 50 U.S.C. § 1802(a)(1)(B), (a)(3) (2006).

256. Davis, *supra* note 242, at 190 (quoting Gerald H. Robinson, *We're Listening! Electronic Eavesdropping, FISA, and the Secret Court*, 36 WILLAMETTE L. REV. 51, 72 (2000)).

257. *See id*. at 196 (noting that the Fourth Amendment's "criminal standard of probable cause" and FISA's "foreign intelligence standard" of probable cause are "very different").

258. *See id.* at 204 (noting that FISA has withstood "substantial judicial scrutiny").

259. *See id.* at 192–93 (describing the requirements of FISA court surveillance applications).

V. A WAY FORWARD—THE MARYLAND MODEL

Even if one understands the case behind each of the interests that will be implicated in a statute limiting police surveillance and intelligence gathering, crafting a statute that satisfies both will be no easy task. Drawing on prior experience may help. This Part suggests one possible model by looking at the legislative response to a past example of police surveillance that occurred in a non-terrorism-related context. The statute discussed in this Part offers both a good starting point for limiting widespread police surveillance, and also some room for improvement to ensure it protects individuals from the much more amorphous intelligence gathering that has occurred in the counterterrorism context.

A. Background

In 2004, as the State of Maryland prepared to execute three prisoners over the next three years,[260] a fierce debate arose in the public sphere over capital punishment in the state.[261] In February 2005, following the execution of the first of those three prisoners, commanders at the Maryland State Police (MSP)[262] began to worry about anti-death penalty activists protesting the two remaining executions and asked for a "threat assessment" from MSP's Homeland

260. The three prisoners were Steven Oken, who was executed in 2004; Wesley Baker, executed in 2005; and Vernon Lee Evans, whose execution was stayed in 2006. Jennifer McMenamin, *Evans' Death Sentence on Hold*, BALT. SUN, Feb. 7, 2006, at 1A; Lisa Rein, *Anticipated Death Penalty Protests Prompted Spying*, WASH. POST, July 26, 2008, at B1; *Capital Punishment History: Persons Executed in Maryland Since 1923*, MD. DEP'T PUB. SAFETY & CORRECTIONAL SERVICES, http://www.dpscs.state.md.us/publicinfo/capitalpunishment/demographics_persons1923.shtml (last visited August 26, 2011) [hereinafter *Capital Punishment in Maryland*]. The executions of Baker and Oken were only the fourth and fifth executions in the state since 1961. *Id.* In 2009, Maryland tightened its death-penalty rules to limit its use to cases in which there is "DNA or other biological evidence, a videotaped confession or a video recording of the crime." Andrea F. Siegel, *Md. Death Penalty Trial Delayed*, BALT. SUN, July 24, 2010, at A6. As of 2011, Baker is the last prisoner to have been executed in Maryland. *Capital Punishment in Maryland*, *supra.*

261. Rein, *supra* note 260. The 2002 election of Governor Robert Ehrlich, a death-penalty supporter, may have added fuel to the fire of the debate. *See id.*; *see also Former Governors: Robert L. Ehrlich, Jr.*, MD. MANUAL ON-LINE: A GUIDE TO MD. GOV'T (March 7, 2012), http://www.msa.md.gov/msa/mdmanual/08conoff/former/html/msa12125.html [hereinafter *Former Governors*].

262. In 2010, the Maryland State Police had 1,439 sworn personnel. MD. DEP'T OF STATE POLICE, 2010 ANNUAL REPORT 8 (2010).

Security and Intelligence Division.[263] After determining that there was a "'potential for disruption' at both executions,"[264] the Division assigned four troopers to work undercover and infiltrate anti-death penalty activist groups for the purpose of gathering information about the groups' future activities, such as protests and rallies.[265]

The undercover troopers' mission began in March 2005[266] and continued for the next fourteen months.[267] The troopers infiltrated protest groups, befriended activists, joined mailing lists, and inquired about protesting tactics, including civil disobedience.[268] At some point during the investigation, the MSP's net also widened to include not just anti-death penalty activists, but also activists protesting the Iraq War, animal-rights advocates, consumers protesting increases in electricity rates, environmentalists, and even a group committed to establishing more bicycle lanes in cities.[269] In total, during the fourteen-month investigation, the MSP collected information and maintained secret files on fifty-three individuals connected with the various activist groups under surveillance.[270]

Despite launching an operation of such considerable length and

---

263. Lisa Rein & Josh White, *More Groups Than Thought Monitored in Police Spying*, WASH. POST, Jan. 4, 2009, at A1; STEPHEN H. SACHS, REVIEW OF MARYLAND STATE POLICE COVERT SURVEILLANCE OF ANTI-DEATH PENALTY AND ANTI-WAR GROUPS FROM MARCH 2005 TO MAY 2006, at 32 (2008), *available at* http://www.governor.maryland.gov/documents/SachsReport.pdf.

264. Rein & White, *supra* note 263.

265. SACHS, *supra* note 263, at 2, 13, 15 & n.10; Gadi Dechter, *Surveillance Was 'Misguided*,' BALT. SUN, Oct. 2, 2008, at 1.

266. SACHS, *supra* note 263, at 13.

267. Nick Madigan, *Spying Uncovered*, BALT. SUN, July 18, 2008, at 1A. During the fourteen-month investigation, the troopers conducted a total of 288 hours of investigation. *Id.*

268. *See* SACHS, *supra* note 263, at 35–37; Bob Drogin, *Spying on Pacifists, Greens and Nuns*, L.A. TIMES, Dec. 7, 2008, at A18. In terms of infiltration, these methods were unquestionably successful. By the time the investigation came to an end in May 2006, *see* SACHS, *supra* note 263, at 1, one of the troopers had attended twenty-nine different meetings, an average of two per month. Drogin, *supra*.

269. Rein & White, *supra* note 263. Although far from an accurate measure, it is worth noting that, by 2008, more than thirty activist groups had filed freedom-of-information requests with the MSP to determine whether they were among the groups that the undercover troopers had infiltrated. Dechter, *supra* note 265. The expanded scope was possible—and perhaps encouraged—because many of the activists' causes overlapped. Rein & White, *supra* note 263.

270. Laura Smitherman, *Ex-Police Chief Defends Spying*, BALT. SUN, Oct. 8, 2008, at 3A.

breadth, the MSP put few controls in place to ensure the operation abided by constitutional protections of civil liberties. Not surprisingly, the investigation soon "spiraled out of control."[271] Although the activist groups under surveillance were "committed to lawful, peaceful protest,"[272] and there was no evidence of "criminal activity or intent on the part of the protesters,"[273] the undercover trooper frequently requested the case remain open and that surveillance continue.[274] MSP commanders rarely, if ever, questioned these requests, and may have even granted such requests for reasons that had nothing to do with the original impetus for the investigation.[275] Nor did MSP commanders take any action to stop the surveillance from expanding beyond the anti-death-penalty groups that were the original targets of the operation,[276] even though they were reading the field reports from the undercover officers on a daily or near-daily basis.[277] The MSP also had few controls in place for handling the information it received from the investigations.[278]

---

271. Rein & White, *supra* note 263.

272. SACHS, *supra* note 263, at 29–31.

273. Madigan, *supra* note 267.

274. Rein & White, *supra* note 263.

275. SACHS, *supra* note 263, at 41. By some accounts, commanders may have seen ongoing surveillance as a chance to give inexperienced troopers a chance at undercover work. *Id.* at 42. Alternatively, the MSP may have seen the program as a chance to breathe new life into the MSP's Homeland Security and Intelligence Division. *See* Rein & White, *supra* note 263. In 2004, the division's headcount had been "whittled" from about sixty-five officers down to twelve; the downsizing came after the police superintendent who had built up the division following the September 11 terrorist attacks was forced out because of corruption charges. To those within the unit, the surveillance mission must have appeared as a chance to do serious police work and prove their worth. *Id.*; *see also* Madigan, *supra* note 267 (reporting an activist's theory that investigations such as the MSP surveillance program helped local law enforcement agencies obtain funding from the federal government).

276. *See* SACHS, *supra* note 263, at 38 (describing how, in interviews after the fact, "MSP commanders . . . could neither recall any contemporaneous discussions about the decision to expand the investigation to include anti-war groups and pacifists, nor could they articulate a sound law enforcement or public safety basis for doing so").

277. *Id.* at 41.

278. The fifty-three individuals on whom the MSP maintained files were labeled as "terrorists" in the MSP's database, Rein & White, *supra* note 263, even though some of those individuals included two Catholic nuns, a congressional candidate, and a man who campaigned against military recruiting at high schools. Lisa Rein, *Spying on Activists Discussed at Forum*, WASH. POST, Oct. 12, 2008, at C3. One of the individuals in the MSP's files had never been to Maryland, while others had been there but were not present in the state when the spying took place. *Id.* Despite a lack of evidence of criminal activity, however, the MSP took no action to remove the information from the database; instead, the

The investigation and the surveillance became public in July 2008 during a separate trespassing trial involving several of the activists,[279] and the demand for a public accounting was almost immediate.[280] Although the MSP asserted that the surveillance was not unlawful, and that the agency did not "inappropriately curtail" the activists' civil liberties,[281] such justifications were short-lived.[282] Within a day, Governor Martin O'Malley vowed to put an end to any police spying conducted without evidence of wrongdoing,[283] and later appointed the former state Attorney General Stephen Sachs to lead an independent review of the MSP's surveillance program.[284]

Conducted over a two-month period in 2008, Sachs's review was thorough—and damning.[285] Following interviews with all of the major players involved,[286] the review concluded that (1) the surveillance program "intruded upon the ability of law-abiding Marylanders to associate and express themselves freely;" (2) the MSP violated federal law by sharing its intelligence with other law enforcement agencies; and (3) the "MSP showed a lack of judgment" by describing peaceful activists as terrorists in various police databases.[287] The review also

information was shared with federal authorities and at least seven different local law enforcement agencies. Rein & White, *supra* note 263.

279. Rein & White, *supra* note 263. The program became public because of documents that were discovered during a trespassing trial for several activists in 2008. *See id.* Subsequent freedom-of-information requests and additional lawsuits compelled the MSP to release additional documents pertaining to the program. *Id.*

280. Jonathan Bor & Gus G. Sentementes, *State Police Spying Decried*, BALT. SUN, July 19, 2008, at 1A.

281. Madigan, *supra* note 267.

282. The surveillance program had been conducted under the administration of Governor Robert Ehrlich, a Republican who was in office from 2003 to 2007. *Former Governors*, *supra* note 261. By the time it became public knowledge, Maryland voters had replaced Ehrlich with Governor Martin O'Malley, a Democrat. *See Governor: Martin J. O'Malley*, MD. MANUAL ON-LINE: A GUIDE TO MD. GOV'T (Sept. 5, 2012), http://www.msa.md.gov/msa/mdmanual/08conoff/html/msa13090.html. If nothing else, O'Malley could easily afford to distance himself from the events of a predecessor's administration because his predecessor came from the opposing political party.

283. Bor & Sentementes, *supra* note 280.

284. Laura Smitherman, *Review of State Police Is Ordered*, BALT. SUN, Aug. 1, 2008, at 1A.

285. *See* SACHS, *supra* note 263; Smitherman, *supra* note 284. Sachs was appointed by Governor O'Malley to lead the review on July 31, 2008, and submitted his final report on Sept. 29, 2008. SACHS, *supra* note 263, at 1, 13.

286. Sachs interviewed MSP commanders, the troopers who conducted the surveillance, and the activists whose organizations were infiltrated. SACHS, *supra* note 263, at 14–15.

287. *Id.* at 3, 6–7.

recommended several corrective actions to the MSP, including adopting regulations to more tightly control surveillance and notifying individuals who were wrongly labeled terrorists in police databases.[288] The MSP subsequently announced it would adopt all of the report's recommendations.[289]

The public, however, demanded its own protections, and in 2009, the Maryland General Assembly passed and Governor O'Malley signed into law the Freedom of Association and Assembly Protection Act of 2009.[290] The law, as well as the regulations adopted pursuant to it,[291] provide for greater controls over police surveillance and intelligence-gathering activities, while still offering police enough leeway to conduct legitimate investigations if the need arises. This is a useful model that other jurisdictions might adopt. The rest of this Part will discuss the law's features and offer some modest recommendations for improvements upon the law.

B. The Law

The Freedom of Association and Assembly Protection Act contains several specific limitations on police conduct that serve to protect individuals' civil liberties. To start, the law's key provision prohibits officers from conducting a "covert investigation" of individuals involved in "First Amendment activities" unless the top official at the agency—for example, the chief of police—finds both (1) a "reasonable, articulable suspicion" that the person is engaged in criminal activity and (2) that a less intrusive method of investigation will not suffice.[292] Within the context of the law, a covert investigation involves attempted or actual infiltration of an organization in which the law enforcement agency or officer's identity is concealed,[293] although the use of plainclothes officers for security purposes at public events is exempt from this definition.[294] First Amendment activities include both constitutionally protected speech as well as conduct related to certain

288. *Id.* at 8–10.

289. Dechter, *supra* note 265.

290. 2009 Md. Laws 2713 (codified at MD. CODE ANN., PUB. SAFETY § 3-701 (LexisNexis 2011)).

291. MD. CODE REGS. 29.08.01.04 (2011); 37 Md. Reg. 432 (Feb. 26, 2010).

292. MD. CODE ANN., PUB. SAFETY § 3-701(c)(1) (LexisNexis 2011).

293. *Id.* § 3-701(a)(3)(i).

294. *Id.* § 3-701(a)(3)(ii).

First Amendment rights such as "free exercise of religion, freedom of the press, the right to assemble, or the right to petition the government."[295]

In addition to the primary limitation described above, the law also restricts police conduct in other ways, several of which are directly applicable to the widespread intelligence-gathering operations established by police after September 11, 2001. First, any investigations involving First Amendment activities must be conducted for a "legitimate law enforcement objective," and in the process of conducting such investigations, police must take measures to "safeguard the constitutional rights and liberties of all persons."[296] Once all leads have been exhausted and no legitimate law enforcement purpose remains, the investigation must be terminated.[297] Police may not collect information solely about a person's "political beliefs, ideologies, and associations" unless it is either relevant to a criminal investigation or there is a reasonable suspicion of certain criminal activities.[298] Finally, any information obtained in violation of the law may not knowingly be included in police intelligence files.[299] Notably, the law also requires local law enforcement agencies in Maryland to have adopted publicly available policies governing their officers' conduct in investigations involving First Amendment activities and their recordkeeping practices for information obtained from such investigations.[300] Typically, such a

295. *Id.* § 3-701(a)(5); *see also* U.S. CONST. amend. I ("Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press, or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.").

296. MD. CODE ANN., PUB. SAFETY § 3-701(d)(1)–(2) (LexisNexis 2011). Legitimate law enforcement objectives are only those involving the "detection, investigation, deterrence, or prevention of crime, or the apprehension and prosecution of a suspected criminal." *Id.* § 3-701(a)(7).

297. *Id.* § 3-701(f).

298. *Id.* § 3-701(g); *see also id.* § 3-701(g)(2) (listing the crimes for which a "reasonable articulable suspicion" allows the police to collect such information).

299. *Id.* § 3-701(k). It is worth emphasizing a law enforcement agency must have *knowledge* that the information they are placing in a criminal intelligence file was obtained in violation of the law, *id.*, which appears to allow for the negligent inclusion of intelligence obtained in violation of the law. But the statute that governs the act of collecting intelligence, *id.* § 3-701(g), contains no such qualifying language, suggesting that in a case of negligent inclusion, a plaintiff could still hold law enforcement liable for collecting the information in the first place.

300. *Id.* § 3-701(m).

policy simply incorporates portions of the law almost verbatim.[301]

As required by the law,[302] the MSP adopted regulations for its practices involving the conduct covered by the law; although these regulations apply only to the MSP, they are useful because they provide additional detail on how a local law enforcement agency is implementing the law. For the most part, the regulations mirror the law, but they expand upon it in certain key respects. For example, whenever a regulated investigation is in progress, officers are required to submit—and commanders are required to review—ongoing reports about the investigations within tightly limited time frames;[303] the purpose of such reports is to provide commanders with a regular opportunity to terminate the investigation if it risks violating the law.[304] Additionally, the MSP must purge criminal intelligence files that no longer have any informational value, and it must annually audit its files to determine whether any of them meet this criteria.[305] Finally, the regulations also contain an important limitation that prevents police from circumventing the regulations by using third parties, such as informants, to obtain regulated information on their behalf.[306]

Because the law has only been in effect since 2009, and the MSP regulations since 2010, it may be too soon to determine whether the law is having its intended effect. Early indications are that it may have been successful; on its website, the American Civil Liberties Union does not list any examples of police spying in Maryland following the MSP incident described in Part V.A.[307] Nevertheless, there are additional civil

---

301. *See, e.g.*, General Orders, Ronald A. Ricucci, Chief of Police, Takoma Park Police Dep't, No. 631A on Covert Investigations (Oct. 1, 2009), *available at* http://www.takomapark md.gov/police/documents/covertinvestigations.pdf. For an example of verbatim text sections, see the identical definition of "covert investigation" in the Takoma Park Police Department General Orders and the Maryland Code. *Compare id.* at 103A, *with* MD. CODE ANN., PUB. SAFETY § 3–701(a)(3)(i) (LexisNexis 2011).

302. MD. CODE ANN., PUB. SAFETY § 3-701(b)(l) (LexisNexis 2011).

303. MD. CODE REGS. 29.08.01.04A(4) (2011) (noting that under this regulation, a report must be submitted by a covert officer within two working days after each contact with the target of the investigation, and such reports must be reviewed by commanders within five working days after the report's submission).

304. *Id.* at 29.08.01.04A(4)(d)–(e).

305. *Id.* at 29.08.01.04B(8)(d), .04B(9).

306. *Id.* at 29.08.01.05B(2).

307. *Spying on First Amendment Activity—State-by-State*, AM. CIVIL LIBERTIES UNION, http://www.aclu.org/maps/spying-first-amendment-activity-state-state (click on Maryland for detail) (last visited Sept. 18, 2012). On the other hand, it may just be that the MSP has gotten better at conducting its covert investigations.

liberties protections that could be incorporated into the law, which are outlined in the next section of this Part.

C. Recommendations for Improvements to the Law

No law is perfect.[308] The Freedom of Association and Assembly Protection Act is the product of the inevitable compromises that are necessary when crafting legislation that walks the fine line between two intensely held interests like protecting civil liberties and securing public safety. Generally, the Act strikes a fair balance between protecting civil liberties (by giving individuals protection against certain types of police conduct) and preserving the ability of police to defend the nation's security (by limiting its civil liberties protections to certain, more sensitive contexts like "First Amendment activities").[309] But as a model statute for other jurisdictions, it would benefit from a handful of amendments that would strengthen its protections without unduly burdening law enforcement.

There are at least six different changes that should be made to the law. The first three changes arise from both what we know about the nature of widespread police surveillance and intelligence gathering,[310] and what we know about the nature of covert investigative power—namely, that it has historically been prone to abuse:[311] Lawmakers should (1) expand the list of activities that trigger the statute's protections; (2) require court approval for any request to circumvent the law; and (3) entrust responsibility for oversight to a third party outside the division conducting the investigations at issue (and preferably outside the law enforcement agency altogether). The other three changes recommend themselves from the FISA, which, though it has weathered its share of due-process criticism,[312] nevertheless contains some basic procedural elements that could benefit the Maryland law as

308. Davis, *supra* note 242, at 178.

309. *See supra* Part V.B.

310. *See supra* Part II.B.

311. *See* Raymond Shih Ray Ku, *Unlimited Power: Why the President's (Warrantless) Surveillance Program Is Unconstitutional*, 42 CASE W. RES. J. INT'L L. 647, 672 (2010) ("One of the fundamental lessons this nation learned is that all power, including investigative powers, is easily abused . . . ."); Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now?: Toward Reasonable Standards for Law Enforcement Access to Location Data That Congress Could Enact*, 27 BERKELEY TECH. L.J. 117, 185 (2012) ("Covert surveillance methods are investigative tools that by their very nature invade the privacy of those targeted and are, as history has shown, prone to abuse.").

312. *See supra* note 256 and accompanying text.

a model statute: Lawmakers should (4) strengthen the law's "minimization procedures"[313] to ensure innocent parties' privacy is preserved; (5) require police to provide regular reports to the city council or state legislature on both the volume and nature of surveillance conducted under the law; and (6) require police to develop training for officers to ensure they understand and will comply with the law's requirements. I will discuss these six recommendations in order.

First, lawmakers should expand the list of activities that trigger the statute's protection by broadening the definition of "covert investigation." The statute currently only includes investigations involving actual or attempted police infiltration,[314] which means that, in its current form, the statute offers little protection against the extended surveillance or data-mining that are characteristic of post-September 11 police intelligence operations, but which do not rely on infiltration. These activities should be included within the law's definition of covert investigation.

Although law enforcement advocates will cry foul, there are three considerations that should ease their concerns. First, the law only applies to investigations involving First Amendment activities, which means surveillance, data-mining, and other investigative tools discussed in this Comment remain freely available in less sensitive contexts.[315] Second, the law arguably already prohibits the use of these tools in First Amendment contexts because it also prohibits the maintenance of criminal intelligence files containing information involving First Amendment activities when that information has no application to a current criminal investigation.[316] Adding such activities to the definition of covert investigation only serves to make the law more explicit, not more burdensome. And, finally, when it comes to gray areas, the courts are likely to give law enforcement the benefit of the doubt.[317]

---

313. *See, e.g.*, 50 U.S.C. § 1801(h) (2006) (defining "minimization procedures" in the context of FISA).

314. MD. CODE ANN., PUB. SAFETY § 3-701(a)(3)(i) (LexisNexis 2011).

315. *Id.* § 3-701(c)(1).

316. *Id.* § 3-701(g).

317. *See* Davis, *supra* note 242, at 178 (arguing that "laws will probably be interpreted to support the government's tendency toward self-preservation when a 'threat to the nation's security is real'" (quoting David G. Savage, *Historically, Laws Bend in Time of War, Rehnquist Says*, L.A. TIMES, June 15, 2002, at A22)); *see also* Harris, *supra* note 80, at 153 ("In today's post-9/11 climate, it is hard to imagine a federal court issuing directives limiting police use of surveillance activities . . . .").

The second change that should be made to strengthen the law is to require judicial approval of any request to circumvent the law's protections, rather than the current requirement that such deviations be authorized by the head of the law enforcement agency conducting the investigation.[318] At most, the agency head's authorization should only be effective in cases of exigent circumstances—and only then until proper judicial authorization can reasonably be obtained. Although law enforcement advocates may argue that this places an additional burden on police, the fact is that requiring judicial approval does not change the requirement that police justify their investigations with a "reasonable, articulable suspicion" of criminal activity—it only changes the person to whom such a justification is made. On the contrary, requiring judicial approval to circumvent the law's protections recognizes that, even when acting in good faith, police have an inherently "stronger interest in investigation" than in avoiding any collateral damage (such as to civil liberties) resulting from those investigations.[319] Positioning the courts as a safeguard provides a counterweight to this interest.

The third change is to give responsibility for oversight to a third party outside of the division of the law enforcement agency conducting the investigation (and ideally out of the police department altogether), because law enforcement agencies are not adept at self-regulation. Normally, self-regulation within law enforcement is driven by public dissatisfaction with police conduct,[320] but in the case of terrorism prevention, the public's insistence that the government do all it can to stop another terrorist attack from occurring may outweigh concerns over civil liberties infringements.[321] Furthermore, past failures by law enforcement to self-regulate may suggest many agencies lack the will to self-regulate.[322] Additionally, even in those cases where law

---

318. MD. CODE ANN., PUB. SAFETY § 3-701(c)(1) (LexisNexis 2011).

319. *See* Andrea L. Dennis, *Collateral Damage? Juvenile Snitches in America's "Wars" on Drugs, Crime, and Gangs*, 46 AM. CRIM. L. REV. 1145, 1189 n.248 (2009).

320. *See* Evan N. Turgeon, *National Security, Policing, and the Fourth Amendment: A New Perspective on* Hiibel, 27 BUFF. PUB. INT. L.J. 23, 49–50 (2008–2009).

321. Elected civic leaders typically must answer to dissatisfied voters at election time, giving them an incentive to ensure that police keep their conduct in line. *See id.* at 50. But if voters send a different message—stop terrorists at all costs, for example—it removes the incentive for elected officials to exert pressure on police, and that protection is lost.

322. *See* Barbara E. Armacost, *Organizational Culture and Police Misconduct*, 72 GEO. WASH. L. REV. 453, 481–82 (2004) ("A pattern of continued wrongdoing that is known but unaddressed . . . suggests that the organization has lost the will and/or the ability to police itself.").

enforcement has self-regulated, these restrictions have often been rolled back post-September 11.[323]

Oversight is better addressed by a third party—either a kind of ombudsman within the agency's internal affairs division, or someone within the local government outside of the police department—who can bring local knowledge of law enforcement priorities as well as independent perspective and judgment to the required review of intelligence files. Law enforcement may balk at such restrictions, but in addition to strengthening civil liberties, oversight may help police become more efficient, in at least two different respects. On one hand, oversight will give police an opportunity to better understand whether particular investigative methods are working.[324] On the other, oversight will help avoid duplication of efforts and eliminate waste, an especially valuable service for police departments that are stretched thin as they try to meet substantial demands with scarce resources.[325]

The fourth change to the law is to strengthen the law's requirement that police implement "minimization procedures"[326] to ensure innocent parties' privacy is preserved. Although the law already requires that police take measures to "safeguard the constitutional rights and liberties of all persons,"[327] in its current form it leaves this responsibility to police. Because police may be unable or unwilling to self-regulate,[328] strengthening the minimization-procedures requirement is essential, and can be accomplished in one of two ways: either the law could require judicial approval of minimization procedures established as part of a widespread surveillance operation,[329] or the law could require that the

323. *See* Harris, *supra* note 80, at 151–52 (describing how restrictions on the use of surveillance in Chicago and New York that were put in place in the 1980s have been rolled back after September 11).

324. *See* Orin S. Kerr, *The National Surveillance State: A Response to Balkin*, 93 MINN. L. REV. 2179, 2183 (2009) (arguing that there is a "natural role for oversight [of surveillance] focused on efficacy. . . . If a surveillance tool or program doesn't work, it shouldn't be used. This seems obvious, but tends to become lost in practice.").

325. *See* Danielle Keats Citron & Frank Pasquale, *Network Accountability for the Domestic Intelligence Apparatus*, 62 HASTINGS L.J. 1441, 1488–89 (2010–2011) (noting the "size and redundancy of the U.S. anti-terror apparatus" and arguing that independent oversight can address the "overall cost-effectiveness" of domestic intelligence spending).

326. 50 U.S.C. § 1801(h) (defining "minimum procedures" in the context of FISA).

327. MD. CODE ANN., PUB. SAFETY § 3-701(d)(2) (LexisNexis 2011).

328. *See supra* notes 321–22 and accompanying text.

329. This type of mechanism has been used in a number of federal laws related to surveillance; in addition to FISA, the Wiretap Act, also requires judicial approval of minimization procedures. Pell & Soghoian, *supra* note 311, at 184.

relevant executive authorities draft rules in advance to specifically define what minimization procedures are required.[330] Because minimization procedures "can and should play a role in limiting the privacy harms associated with" covert investigations, strong rules governing such procedures are essential to the law's effectiveness.[331]

The fifth change lawmakers should make to the law is to require police to regularly file publicly available summary reports on the nature and volume of regulated investigations they have conducted. Such reports could be modeled on those mandated by FISA, which requires the Attorney General to report to Congress every six months on various aspects of covert investigations.[332] Ideally, these reports will provide the public with the information they need to assess whether police conduct conforms to the public's expectations,[333] while remaining nonspecific enough to avoid compromising ongoing investigations. Any police conduct that is uncovered through these reports but does not conform to the public's expectations can be averted through further legislative amendments, mitigating long-term damage to Americans' privacy interests.[334]

The sixth and final change to be made to the law involves requiring police to develop training for officers to ensure they understand and will comply with the law's requirements. While this is perhaps the most functional and least strategic of the proposals outlined here, it

---

330. As part of the USA PATRIOT Act, "Congress directed the [Department of Justice] to adopt specific minimization procedures for records obtained pursuant to" certain regulations related to national security. *Id.* at 184–85. Although some may argue this is still a form of self-regulation, drafting the rules in advance may at least limit the most blatant cases of manipulation.

331. *See id.* at 184.

332. 50 U.S.C. § 1871(a) (2006). Among other data, the Attorney General must provide Congress with a breakdown of the number of persons targeted by various types of investigations, *id.* § 1871(a)(1), the number of times the Attorney General has authorized the use of intelligence acquired under FISA in a criminal proceeding, *id.* § 1871(a)(3), and any significant legal interpretations stemming from FISA-related court proceedings, *id.* § 1871(a)(4).

333. *See* Pell & Soghoian, *supra* note 311, at 188–89 (detailing the public benefits of reporting requirements in various federal laws related to surveillance, such as allowing the media to report on the government's increased use of wiretaps and scholars to study trends in government surveillance practices).

334. *See* Stephanie Cooper Blum, *What Really Is at Stake with the FISA Amendments Act of 2008 and Ideas for Future Surveillance Reform*, 18 B.U. PUB. INT. L.J. 269, 303 (2009) (asserting that "ex post oversight mechanisms" in FISA, as amended in the FISA Amendments Act of 2008, 50 U.S.C. § 1881, "might mitigate the risk that innocent Americans' communications will be acquired and retained").

nevertheless serves an important role in making the law an effective barrier to the abuse of widespread surveillance powers. Ideally, legislatures and city councils would continue to reevaluate the law's provisions,[335] but because this may not always be possible, the next-best option may be police departments staffed by officers who are well acquainted with the legislative intent, and the surveillance that is permitted within the law's boundaries.[336] Additionally, similar to FISA, the law might include provisions that restrict officers from participating in regulated investigations until they have received the required training, and that the effectiveness of training be evaluated by the head of the department or a third-party ombudsman on a regular basis.[337]

Taken together, these proposals should result in a model statute that provides strong and durable oversight over widespread police surveillance and intelligence gathering—at least in sensitive contexts such as those regulated by the First Amendment—while still allowing police the capability to preemptively track and disrupt potential terrorist organizations. In the final section of this Part, this Comment will return to the cases in Los Angeles and New York City, discussed earlier, to assess whether the law might truly be effective.

D. Applying the Law—How Things Might Have Been Different

The cases in New York City[338] and Los Angeles[339] discussed in Part II.B. provide typical examples of the type of widespread police surveillance and intelligence gathering with which this Comment is concerned. In closing, the final section of this Part will attempt to illustrate how an amended version[340] of the Maryland Freedom of Association and Assembly Protection Act might have mitigated police conduct and protected civil liberties in those cases (and others like

335. *See* Charles A. Shanor, *Terrorism, Historical Analogies, and Modern Choices*, 24 EMORY INT'L L. REV. 589, 606 (2010) (arguing that ongoing legislative rulemaking is the best solution for intelligence oversight, in the long run superior to either judicial process or an unregulated executive).

336. *See, e.g.*, Blum, *supra* note 334, at 303 (highlighting the requirement imposed by the FISA Amendments Act of 2008, 50 U.S.C. § 1881a(f)(1), that intelligence personnel be trained in the implementation of FISA's restrictions as an effective way to mitigate the risks FISA poses to Americans' civil liberties).

337. *See* Blum, *supra* note 334, at 303.

338. *See supra* Part II.B.2.

339. *See supra* Part II.B.1.

340. For the purposes of this section, I will assume the law has been amended and strengthened in accordance with the proposals outlined in Part V.C.

them), had the law been in place in each jurisdiction.

The most important protection that the law would have provided is that widespread surveillance and intelligence-gathering operations, like those conducted by the LAPD and NYPD, would have qualified under the law as "covert investigations," and thus become subject to the law's regulations.[341] As a result, the investigations could not have proceeded—at least with respect to First Amendment activities such as the free exercise of religion or peaceable assembly—without judicial authorization.[342] To obtain such an authorization, police would have had to argue before a judge that there was both a "reasonable, articulable suspicion" of criminal activity, and that no less intrusive investigative method would satisfy police objectives.[343] All of these procedural hurdles would have provided opportunities to stop, limit, or better control the investigations.

Assuming, *arguendo*, that courts decided the LAPD and NYPD intelligence-gathering operations satisfied this standard and allowed police to continue, authorities would still have had to comply with the law's other oversight mechanisms. For example, police would have been required to compile minimization plans to ensure that innocent members of the public saw their privacy rights preserved, and such plans would have either required judicial approval, or must have complied with the guidelines established by authorities in advance.[344] Furthermore, police would either be prohibited from maintaining intelligence files on information gathered through these investigations (if the information was gathered in violation of the law), or police would have been required to purge the information when regular audits revealed that it no longer had any informational value to an ongoing investigation.[345]

In addition, police would have had to regularly file reports—either

341. *See supra* notes 314–17 and accompanying text.

342. *See supra* note 318 and accompanying text.

343. *See supra* note 292.

344. *See supra* notes 327–31 and accompanying text. Minimization procedures would have been useful in both cases. The NYPD almost certainly gathered intelligence on innocent individuals through undercover police reports on everyday activities at cafés, restaurants, and other public locations. *See supra* notes 86–87 and accompanying text. The LAPD's current suspicious-activity reporting program, which allows police to report their observations of innocuous activity without any independent suspicion of wrongdoing, likely has the same result. *See supra* notes 72–73 and accompanying text.

345. *See supra* notes 304–05 and accompanying text.

to the city council, the state legislature, or some other independent oversight commission, depending on how the law was drafted—on the volume and type of surveillance they were conducting, which would provide the public with additional opportunities for oversight.[346] In cases of widespread surveillance and intelligence gathering like those in New York City and Los Angeles, this might have offered the public a glimpse of both programs before they triggered public outrage, and given police a chance to better consult with residents on how best to achieve their objectives while respecting civil liberties.[347]

Finally, with a law like the amended version of the Maryland Freedom of Association and Assembly Protection Act in place—and the greater awareness of the delicate balance between national security and civil liberties that would come with the law's control mechanisms[348]—it is possible that police might have decided to devise an entirely different type of counterterrorism intelligence program. But the more important point is that, with these control mechanisms in place, the public would be better poised to respond with flexible, dynamic laws and regulations to preserve privacy while still addressing national security. As can be seen, this approach has a number of advantages over more static constitutional remedies like those in the Fourth Amendment.

VI. CONCLUSION

In our current political climate, the nation's collective thumb is indeed pressing on the scale in the direction of national security.[349] The population demands protection from further terrorist attacks and insists that the devastation of September 11, 2001, not be allowed to repeat itself. The government has responded, making funding available to police forces across the country and encouraging them to serve as the front line in the war on terror, even if at the expense of civil liberties. But, though we may have asked for such measures, we are not subsequently prevented from unasking them in the interest of protecting our civil liberties. This Comment has discussed two significant ways this

346. *See supra* notes 332–33 and accompanying text.

347. Police appear to have attempted this, somewhat belatedly, in Los Angeles. *See supra* note 69. In New York, however, the surveillance program appears to have been kept much more secret, with no attempt at community engagement. *See* Hawley, *supra* note 89.

348. *See supra* Part V.C for an outline of the proposed control mechanisms, such as third-party oversight, regular reporting of surveillance activities, and in-depth training for officers involved in intelligence-gathering operations.

349. *See supra* note 190 and accompanying text.

might occur. One—the Fourth Amendment—may not offer much hope for individuals, while the other—statutory limits—appears more promising. The so-called Maryland model discussed in Part V is only one example of such a statute, but the specific form and substance of such a statute, and even whether a statute is the best corrective method, will be left to the decision makers of the future. It is imperative, however, that a decision be made. Surveillance and intelligence-gathering methods and technologies will only become more covert, more invasive, and more economically feasible. Taking the easy way out—punting these decisions another thirty years into the future—is to risk allowing the issue to bypass us altogether, such that the use of these tactics may become so pervasive that we will truly miss our chance to opt out.

Craig Roush*

* Candidate for J.D., 2014, Marquette University; M.B.A., 2012, Marquette University; B.F.A., 2004, New York University. Thank you to Dean Michael O'Hear, Prof. Chad Oldfather, Sabrina Stephenson, and Loren Peterson for either providing input on this topic or reading through earlier drafts and providing helpful and constructive criticism. Thank you to the staff of the *Marquette Law Review*, for your tireless work behind the scenes. Thank you to my parents, Craig Roush and Renée Rudolph, who taught me everything I know and made me the person I am today. And, finally, thank you to my wife, Kirsten—you have continually encouraged me to do great things and believe in myself while doing them. Your generous measures of love and patience are just what I need but more than I deserve; and if I never fully repay the favor, it will not be for lack of trying.