## NOTE

# NO CAUSE OF ACTION: VIDEO SURVEILLANCE IN NEW YORK CITY

*Olivia J. Greer*[*]

Cite as: *No Cause of Action: Video Surveillance in New York City*, 18 MICH. TELECOMM. TECH. L. REV. 589 (2012), *available at* http://www.mttlr.org/voleighteen/greer.pdf



### INTRODUCTION

In 2010, New York City Police Commissioner Raymond Kelly announced a new network of video surveillance in the City. The new network would be able to prevent future terrorist attacks by identifying suspicious behavior before catastrophic events could take place. Kelly told reporters, "If we're looking for a person in a red jacket, we can call up all the red

[*] Acquisitions Editor, Cardozo Arts & Ent. L.J. (2011–2012); J.D. candidate, Benjamin N. Cardozo School of Law, 2012; B.S., Skidmore College, 2003. Thanks to Professor Susan Crawford for her expertise, guidance, and tremendous support, and to Molly Storey, Julie Bernard, and the editors of this Journal.

jackets filmed in the last 30 days,"[1] and "[w]e're beginning to use software that can identify suspicious objects or behaviors."[2] *Gothamist* later made a witticism of Kelly's statement, remarking, "Note to terrorists: red jackets are *not* a good look for you."[3] This small joke captured a real concern for New Yorkers: what if you're not a terrorist, but you do happen to wear a red jacket in the subway on a day when the New York City Police Department is looking for red-jacketed terrorists? And what if you happen to have brown skin? Or pray at a mosque? Should these attributes be captured on video, are they sufficient for the NYPD to bring you in for questioning, or even to arrest you?

Surveillance cameras have been present in New York City for decades, installed and monitored by both the NYPD and private business owners.[4] After September 11th and the PATRIOT Act, their numbers surged.[5] The number of cameras that capture the images of New Yorkers each day remains dwarfed by those in London, where there is one camera for every fourteen residents,[6] under the much-celebrated and equally controversial "ring of steel."[7] However, the numbers in New York are in the thousands,

---

1. John Del Signore, *NYPD Tightens Surveillance in Subway's "Ring of Steel*," GOTHAMIST (Sept. 21, 2010), http://gothamist.com/2010/09/21/nypd_tightens_surveillance_in_subwa.php.

2. *Id.*

3. *Id.*

4. *See generally A History of Surveillance in New York City*, NOT BORED!, http://www.notbored.org/nyc-history.html (last visited Jan. 15, 2012). *Not Bored!* is an irregularly published online journal associated with the Surveillance Camera Players that has adopted the concept of "surveillance art," the use of technology to record human behavior, in a way that offers commentary on the process of surveillance or the technology used to surveil. The Surveillance Camera Players tracked video surveillance in New York City from 1996 to 2006. *The Surveillance Camera Players*, NOT BORED!, http://www.notbored.org/the-scp.html (last visited Feb. 13, 2012); *see also* Leah Borromeo, *Tate Makes Surveillance an Art Form*, COMMENT IS FREE: LIBERTY CENT. (May 28, 2010, 9:30 AM), http://www.guardian.co.uk/commentisfree/libertycentral/2010/may/28/tate-modern-surveillance-art; Hugh Hart, *The Art of Surveillance*, WIRED, (Nov. 30, 2007), http://www.wired.com/culture/art/multimedia/2007/11/gallery_surveillance_art (beginning of a series of images of artistic surveillance devices over multiple pages).

5. *See, e.g.*, Del Signore *supra* note 1; Henry Goldman, *New York City Police Will Monitor 500 More Cameras, Bloomberg Says*, BLOOMBERG (Sept. 20, 2010), http://www.bloomberg.com/news/2010-09-20/new-york-city-will-get-500-more-subway-cameras-under-surveillance-system.html; *see also* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Pub. L. No. 107-56, 115 Stat. 272 (2001) (codified in scattered titles and sections of U.S.C.) (authorizing enhanced surveillance procedures and other domestic security measures).

6. Max Guirguis, *Electronic Visual Surveillance and the Reasonable Expectation of Privacy*, 9 J. TECH. L. & POL'Y 143, 146 (citing Andrea Thompson, *Big Brother UK*, DAILY MAIL, Jan. 23, 2004, at 24).

7. There is wide disagreement on the effectiveness of the "ring of steel." *See* Cara Buckley, *Manhattan Takes Cue from London's "Ring of Steel"* N.Y. TIMES, Jul. 9, 2007, at A1 (reporting on the earliest implementation of the Lower Manhattan Security Initiative, comparing it to the "ring of steel" and noting that the "ring of steel" was unable to prevent the 2005 subway bombings in London); Kieran Long, *So Can the Secret Ring of Steel Save the*

particularly since the launch of the system announced by Commissioner Kelly in 2010: the Lower Manhattan Security Initiative and the Midtown Manhattan Security Initiative (LMSI and MMSI, respectively).[8] The NYPD touts the LMSI and MMSI as unique: they form a completely networked system, such that all video camera feeds can be monitored from a single location, in real time.[9] This type of program is anticipated to be more effective in stopping crime and terror attacks than London's static system, which provides only playback capabilities and not real-time monitoring.[10] Despite their reach, however, neither the New York nor the London program has yet been proven effective in preventing either crime or terrorist attacks.[11]

Any surveillance program clearly raises privacy concerns for the monitored population. This Note weighs some of those concerns for New Yorkers, not against national security interests, the validity of which this Note largely concedes, but rather against the lack of legal accountability built into the LMSI and MMSI. That is, this Note asks whether the possible encroachments on privacy and the risks of abuse can be justified by a system that was implemented with no legally binding process for accountability to the public, thus bearing the risk of serious privacy violations and abuses. This Note takes the position that, while a surveillance program like New York City's may be justified and needed in the modern world, it cannot be allowed to operate outside of any legally enforceable systems of accountability.

Part I of this Note will offer an overview of video surveillance programs and the conflicting information regarding their efficacy in preventing and solving crime. Part II examines the present state of the City and the law regarding video surveillance in New York City. It also contrasts the NYPD's privacy guidelines for the LMSI and MMSI with the laws governing video surveillance in the United Kingdom, where video surveillance was adopted early and has been used extensively, in London and in other cities and villages. Part III seeks to understand why Chris Dunn, Associate Legal

---

*City from Terrorism?*, London Evening Standard (Oct. 15, 2010), http://www.thisislondon.co.uk/lifestyle/article-23888163-so-can-the-secret-ring-of-steel-save-the-city-from-terrorism.do (reporting on a study of the "ring of steel" and citing the study's assertion that the surveillance program is "is highly unlikely to prevent bomb attacks by individual pedestrians"); Jeffrey Rosen, *A Watchful State*, N.Y. Times Mag., Oct. 7, 2001, at 38 (arguing that, rather than preventing crime, cameras in the United Kingdom, including the "ring of steel," are used to produce "social conformity").

8. Press Release, N.Y.C. Police Dep't, New York City Police Department Releases Draft of Public Security Privacy Guidelines for Public Comment (Feb. 25, 2009), *available at* http://www.nyc.gov/html/nypd/html/pr/pr_2009_005.shtml [hereinafter NYPD Press Release].

9. Anonymous Interview (Oct. 27, 2010) (on file with author) [hereinafter Anonymous Interview] (This interview was conducted with a New York City official who is very close to the LMSI/MMSI and who was not authorized by the NYPD to speak publicly about these programs.); *see also* Del Signore, *supra* note 1.

10. Anonymous Interview, *supra* note 9.

11. *See* Buckley, *supra* note 7; Guirguis, *supra* note 6; Long, *supra* note 7; Rosen, *supra* note 7.

Director of the New York Civil Liberties Union (NYCLU), is convinced that there is no legal argument that could directly challenge the presence of surveillance cameras in New York City.[12] It will identify the types of problems that may stem from New York City's current system, demonstrating very real concerns about privacy invasion and other possible abuses. Part IV will make projections as to where law and practice is heading on this issue, and will posit recommendations and hopes for future practice.

## I. The Effectiveness Question

This section presents a brief overview of the conflicting evidence regarding the effectiveness of video surveillance in preventing crime. The overview is included for two reasons. The first is to draw a context for the discussion that follows, to make clear that citizens are being asked to compromise their privacy interests and risk abuse for the sake of a system whose effectiveness in making them safer is not clearly established. The second reason is to compare most existing video surveillance programs with New York City's relatively new Lower Manhattan and Midtown Manhattan Security Initiatives (LMSI/MMSI) discussed in detail in Part II. These initiatives are on the cutting edge of surveillance technology. But, as will become clear, while their scope is substantially broader, and their capacity for effective, real-time crime prevention may prove to be greater, the privacy and abuse concerns they raise are much the same as they always have been, and may expand as their technological reach expands.

Cameras are championed by government and law enforcement leaders, as well as, in some cases, the general public, as a necessity to protect against terrorist attacks and other crime.[13] There is evidence available to support the assertion that crime rates have fallen in a number of cities following the installation of video surveillance programs.[14] However, as the NYCLU points

12. Interview with Chris Dunn, Assoc. Legal Dir., N.Y. Civil Liberties Union (Oct. 5, 2010) [hereinafter Dunn Interview].

13. An example of a seemingly uncontroversial and effective video surveillance program is in the city of Northampton in the United Kingdom:

> [O]ne of England's earliest surveillance systems was installed at the insistence of the public and was even partially paid for by local businesses. That was the system of the historic city of Northampton, which was introduced in the early 1990s in the wake of the IRA intense bombing campaigns. . . . Both short- and long-term results were quite impressive. The cameras led to seventeen arrests the same month they became fully operational. Two and a half years after the system's installation, police have solved 85% of all crimes in the monitored areas. By the mid-1990s, Northampton's crime record had been cut by 57%.

Guirguis, *supra* note 6 at 147.

14. In the 1990s, crime declined in Tacoma, Washington, by thirty-five percent in the first year cameras were installed; in New York City, crime rates in public housing projects declined by between thirty and fifty percent over five years when cameras were installed; in

out, the cited evidence does not clearly point to surveillance programs as the sole or primary cause of drops in crime rates, at least in New York.[15] Many video surveillance programs were developed and installed in the 1990s, when crime rates were already consistently decreasing, largely due to an expanded police force with an increased physical presence on the streets.[16] In 2006, in testimony before the New York City Council, the NYPD touted its Video Interactive Patrol Enhancement Response (VIPER) program,[17] claiming that, after security cameras were installed in City housing projects, monitored buildings experienced a thirty-six percent drop in crime from the previous year.[18] Anecdotal evidence indicates that the cameras may have contributed to at least some decrease in petty crime, and some residents—and especially managers—of monitored housing projects registered satisfaction.[19] However, no evidence has been presented that directly connects the presence of the cameras to the drop in crime in those areas.[20]

Similarly, in 2003, Congress directed the federal General Accounting Office (GAO) to investigate the effectiveness of video surveillance.[21] The GAO studied four American cities[22] using video surveillance and concluded that there was simply not enough available evidence to conclusively determine whether the cameras were preventing crime.[23] Such findings have been echoed in the United Kingdom. England's Home Office released a survey in 2005, evaluating thirteen local video surveillance programs. The study found a statistically significant reduction in crime in only one of the thirteen

---

Redwood City, California, crime rates dropped eleven percent in the first year and thirty-three percent in the second year after cameras were installed. *Id.* at 147–48.

15. N.Y. Civil Liberties Union, Who's Watching? Video Camera Surveillance in New York City and the Need for Public Oversight 5 (2006) [hereinafter Who's Watching?].

16. *Id.*

17. *Id.* A commanding officer of the NYPD's Technical Assistance Response Unit reported that the VIPER program had placed 3,100 cameras in fifteen public housing buildings managed and monitored by the NYPD and the New York City Housing Authority in 1997.

18. *Id.*

19. Zaheer Cassim, *Public Housing Residents Happy with Close Surveillance*, The Uptowner (Oct. 13, 2010), http://theuptowner.org/2010/10/13/public-housing-residents-happy-with-close-surveillance.

20. Who's Watching?, *supra* note 15, at 5.

21. U.S. Gov't Accountability Office, GAO-03-748, United States General Accounting Office: Video Surveillance: Information on Law Enforcement's Use of Closed-Circuit Television to Monitor Selected Federal Property in Washington, D.C. (2003).

22. *Id.* at 3 (listing Baltimore, Maryland; Tampa, Florida; Columbia, South Carolina; and Virginia Beach, Virginia).

23. *Id.* at 29 ("There is general consensus among CCTV users, privacy advocates, researchers, and CCTV industry groups that there are few evaluations of the effectiveness of CCTV in reducing crime, and few jurisdictions are keeping data to demonstrate that their CCTV systems are effective.").

areas under surveillance, and seven areas had actually experienced increased crime.[24]

In addition to the doubts with regard to the effectiveness of surveillance cameras in preventing everyday crime, there is also a lack of evidence supporting the position that surveillance cameras prevent terrorism.[25] While there are video recordings of some of the actions of the September 11th hijackers prior to the attacks, those video cameras were unable to prevent the attacks.[26] Likewise, London's "ring of steel" video surveillance program in its public transport system also failed to prevent the deaths of fifty-six people in the July 2005 terrorist attacks.[27] As *Business Week* sharply pointed out, following the 2005 attacks in London:

> Lost in the recent London bombings, along with innocent lives, was any illusion that today's surveillance technology can save us from evildoers. Britain has 4 million video cameras monitoring streets, parks, and government buildings, more than any other country. London alone has 500,000 cameras watching for signs of illicit activity . . . . Fanatics bent on suicide aren't fazed by cameras. And even if they are known terrorists, most video surveillance software won't pick them out anyway.[28]

Cameras capture events, and in some cases those images will later help investigators identify the perpetrators of criminal acts. But cameras are by no means a magic bullet. Highlighting the need to prioritize uses of limited resources in New York City, the NYCLU has recognized that "[c]ameras cannot prevent bad things from happening—and the money spent on them may, in fact, divert resources from more effective crime prevention strategies and tactics."[29]

## II. The State of the City

### A. *The Lower Manhattan and Midtown Manhattan Security Initiatives*

Effective or not, video surveillance appears to be with New Yorkers to stay. In 2007, New York launched the Lower Manhattan Security Initiative (LMSI), which includes an integrated network of publicly and privately

---

24. Martin Gill & Angela Spriggs, Home Office Research Study 292, Assessing the Impact of CCTV, at vi (2005), *available at* https://www.cctvusergroup.com/downloads/file/Martin%20gill.pdf; Who's Watching?, *supra* note 15, at 6.

25. Who's Watching?, *supra* note 15, at 6.

26. Sewell Chan, *U.S. Transit Agencies Turn to Cameras in Terror Flight, but Systems Vary in Effectiveness*, N.Y. Times, July 14, 2005, at A1.

27. Who's Watching?, *supra* note 15, at 6.

28. Catherine Yang, *The State of Surveillance*, Bloomberg Businessweek (Aug. 8, 2005), http://www.businessweek.com/magazine/content/05_32/b3946001_mz001.htm.

29. Who's Watching?, *supra* note 15, at 6.

owned cameras, as well as license plate readers, concentrated below 14th Street.[30] In 2010, the city launched a companion program—the Midtown Manhattan Security Initiative (MMSI).[31] Presently, the City is continuously scanning at least 1,159 public and private cameras; it has added 500 new cameras to subway systems in the city and has plans to add approximately 1,800 more image-capturing devices in lower and midtown Manhattan.[32] These cameras record the images of many New Yorkers, multiple times per day.[33] The purpose of LMSI/MMSI is a compelling one: to "aid in the detection of preparations to conduct terrorist attacks,"[34] to "deter terrorist attacks,"[35] and to "reduce incident response times."[36] The programs are run by the NYPD's Counterterrorism Bureau, with primary financial support and some operational oversight from the federal Department of Homeland Security.[37] Distinct in purpose, function, and management from the NYPD's anti-crime programs like VIPER, LMSI/MMSI was created solely to keep New York City safe from future terrorist attacks.[38]

The LMSI area of surveillance extends from Canal Street to the lowest point in Manhattan, and from the East River to the Hudson River.[39] The MMSI area of surveillance reaches from 30th Street to 60th Street, river to

30. Cara Buckley, *Police Plan Web of Surveillance for Downtown*, N.Y. TIMES, July 9, 2007, at A0.

31. Press Release, Office of the Mayor, Mayor Bloomberg, Police Commissioner Kelly, and MTA Chairman Walder Activate Security Cameras Inside Times Square, Penn Station, and Grand Central Subway Stations as Part of NYPD's Midtown Manhattan Security Initiative (Sept. 20, 2010), *available at* http://www.nyc.gov/portal/site/nycgov/menuitem.c0935b9a57bb4ef3daf2f1c701c789a0/index.jsp?pageID=mayor_press_release&catID=1194&doc_name=http%3A%2F%2Fwww.nyc.gov%2Fhtml%2Fom%2Fhtml%2F2010b%2Fpr399-10.html&cc=unused1978&rc=1194&ndi=1 [hereinafter Mayor's Office Press Release].

32. *Id.*

33. Brad Hamilton, *Hidden Eyes of Our Apple; No Escaping City Security Cameras*, N.Y. POST (May 2, 2004), http://www.nypost.com/p/news/hidden_eyes_of_our_apple_no_escaping_GPFusGUurrt1WFF4Pb6ufM ("To see just how often the average New Yorker is caught on film, a *Post* reporter spent the day gathering images from some of the 200 or so cameras he passed during a typical Tuesday on the job. It started early—at 9:51 a.m., when he got coffee at the deli around the corner from his Carroll Gardens, Brooklyn, apartment. About an hour later, he was captured driving on the BQE at Sackett Street by a Department of Transportation traffic cam[era]. From there, he was spotted almost constantly: walking into the newspaper's building on Sixth Avenue in Midtown, riding the elevator to his office, meeting a source in Times Square, talking on the street, eating lunch, taking the subway, having a drink with a pal, renting a DVD. A mix of public and private cameras tracked him moment by moment doing a host of mundane activities.").

34. New York City, N.Y., N.Y.C. Police Dep't Pub. Sec. Privacy Guidelines (Apr. 2, 2009), *available at* http://prtl-prd-web.nyc.gov/html/nypd/downloads/pdf/crime_prevention/public_security_privacy_guidelines.pdf [hereinafter NYPD Guidelines].

35. *Id.* at 3.

36. *Id.*

37. Anonymous Interview, *supra* note 9.

38. *Id.*

39. *Id.*

river.[40] The programs consist of a fiber optic ring around Manhattan that carries the data collected from all of the cameras currently in the network.[41] Through the Lower Manhattan Security Coordination Center, video feeds are pulled in from multiple sources, including NYPD-owned wireless cameras in "high risk" areas (such as the Financial District), "Stakeholder"-owned cameras (private sector "stakeholders" include Goldman Sachs, the New York Stock Exchange, and the Manhattan Transportation Authority), license plate readers, and 911 reports.[42] Personnel from the NYPD, Port Authority, and stakeholder entities all monitor these video feeds and other sources from within the Coordination Center.[43]

What makes LMSI/MMSI unique—and distinguished from the "ring of steel" and other surveillance programs—is that it allows the use of "real-time video analytics."[44] All cameras in the two programs are networked to one dedicated fiber optic ring; one data center processes and stores all of the video footage gathered by the cameras.[45] These characteristics make the network useful for both investigative purposes and—of most interest to the NYPD and its stakeholders—preventative purposes as well.[46] The term "real-time video analytics" refers to a programmable network, which can be built to recognize and flag—in real-time—scenarios such as abandoned packages in the subway.[47] According to the Mayor's office, when fully configured, the analytics can alert police in real-time to a variety of potentially suspicious objects or activities, including unattended parcels, movement in restricted areas, and unusual loitering, and enables investigators to search multiple cameras simultaneously to retrieve incidents of concern.[48] What the Mayor's office has not addressed are questions about the system's operation and the lack of enforceable guidelines to limit potential abuse.

### B. *Public Security Privacy Guidelines*

In 2009, the NYPD released a set of *Public Security Privacy Guidelines* ("*Guidelines*") that purportedly established "policies and procedures to limit the authorized use of the Domain Awareness System and to provide for limited access to and proper disposition of stored data" and to ensure "privacy

40. *Id.*
41. *Id.*
42. *Id.*; Mayor's Office Press Release, *supra* note 31.
43. Mayor's Office Press Release, *supra* note 31.
44. Anonymous Interview, *supra* note 9.
45. *Id.*
46. *Id.*
47. *Id.* London's "ring of steel" is distinguished because it is decentralized, not monitored in real-time, and therefore only useful for post-incident investigations. In the event of an incident, the footage from each camera must be viewed and analyzed separately and manually.
48. Mayor's Office Press Release, *supra* note 31.

protections."[49] The NYPD adopted the *Guidelines*, taking into consideration the "magnitude" of the new system, the large amounts of time, effort and funding that would be invested in new camera technology and implementation of the system, as well as "valid concerns about these systems, governing retention, use, and sharing of video data."[50] The *Guidelines* note that the Domain Awareness System, which encompasses the LMSI and the MMSI, was created under the NYPD's plenary power to protect the public, set out in New York City's Charter.[51] The key objectives of the Domain Awareness System, according to the *Guidelines*, are to: observe the pre-operational activity of terrorist organizations; detect preparations to conduct terrorist attacks; deter terrorist attacks; provide "a degree of common domain awareness" for all of the stakeholders in the LMSI/MMSI; reduce incident response times; and "create a common technological infrastructure to support the integration of new security technology."[52]

The *Guidelines* set out directives aimed at preventing privacy violations that focus on the operation of the system and on the storage, usage, and sharing of data.[53] Generally, operators of the surveillance system are compelled to refrain from biased targeting, to monitor only areas in which no reasonable expectation of privacy exists, to refrain from the use of facial recognition technology, and to require identifying signs on NYPD- and stakeholder-owned cameras.[54] Additionally, the *Guidelines* state that their provisions are to be extended to cases where technologies governed by the *Guidelines* either utilize or are integrated with systems deployed by other divisions of the NYPD.[55] Regarding data, videos are to be stored for only thirty days under ordinary circumstances, and data is to be destroyed after that period.[56] Other types of data, however, may be held for up to five years, or even indefinitely.[57] Decisions to retain data beyond the thirty-day period must be made by an "Authorized Agent," typically either the Deputy Commissioner of Counterterrorism or the Deputy Commissioner for Legal

49. NYPD Guidelines, *supra* note 34 at 1–2 (The "Domain Awareness System" refers to the city's video surveillance system, specifically, "NYPD-owned and Stakeholder-owned closed circuit television cameras (CCTVs) providing feeds into the Lower Manhattan Security Coordination Center; License Plate Readers (LPRs); and other domain awareness devices, as appropriate.").

50. Anonymous Interview, *supra* note 9.

51. NYPD Guidelines, *supra* note 34, at 1; 18 N.Y.C. CHARTER § 435(a) (2011).

52. NYPD Guidelines, *supra* note 34, at 2–3.

53. *Id.* at 3–6.

54. *Id.* at 3.

55. *Id.*

56. *Id.* at 3–4.

57. *Id.* at 2, 4 (Data covered in the *Guidelines*, other than video data, is described as "Metadata," "information about data . . . that increases the usefulness of that data"; "LPR Data," "license plate data collected by fixed or mobile LPR devices"; and "Environmental Data," "environmental data collected by devices designed to detect hazards related to potential terrorist threats, or to respond to terrorist attacks.").

Matters.[58] "Data usage" is authorized to further the purposes set out by the *Guidelines*, as well as "in furtherance of legitimate law enforcement and public safety purposes beyond the scope of those purposes set out in the Statement of Purpose."[59] The *Guidelines* state that it is the NYPD's policy "to place limits on the sharing of data with third parties" and to ensure that data is used only for law enforcement purposes.[60] Once again, only an Authorized Agent may approve the sharing of data.[61] Finally, the *Guidelines* provide security protocols to safeguard stored data by limiting access to the Lower Manhattan Security Coordination Center, screening stakeholder representatives, and requiring both NYPD personnel and stakeholder representatives to "complete privacy training . . . with periodic assessments."[62]

The *Guidelines* state that the system will be operated "only in furtherance of legitimate law enforcement and public safety purposes"[63] and express concern for the public's interest in privacy.[64] However, the NYPD and the *Guidelines* make it clear that "flexibility" is required to protect the public, and are very unclear with regard to how much and what type of flexibility is required.[65] Regarding both operations and the treatment of data, the *Guidelines* set out general requirements, but leave substantial room for changes in ordinary operation, with imprecise regulations regarding how such decisions are to be made. For instance, one objective of the Domain Awareness System is to provide infrastructure to support the integration of new security technology, but the possible types of new technology are undefined; and, while the *Guidelines* state that facial recognition technology will not be deployed, it is not clear that this assurance will be lasting.[66] Further, technologies governed by the *Guidelines* may utilize or be integrated with systems and technologies that go undefined, deployed by other bureaus and divisions of the NYPD that also remain undefined.[67] Of overarching concern is the fact that the *Guidelines* allow data to be used for indeterminate "legitimate law enforcement and public safety purposes" beyond the scope of the Statement of Purpose.[68] This effectively means that data may be used for any purpose identified by the NYPD to relate to law enforcement, but not encompassed in the *Guidelines*. Perhaps the most troubling aspect of the *Guidelines* appears in the final paragraph: a disclaimer that states,

58. *Id.* at 3–4.
59. *Id.* at 4.
60. *Id.* at 5.
61. *Id.*
62. *Id.* at 6–7.
63. *Id.* at 4.
64. *Id.* at 1.
65. Anonymous Interview, *supra* note 9.
66. NYPD Guidelines, *supra* note 34, at 3.
67. *Id.*
68. *Id.* at 4.

"[n]othing in these *Guidelines* is intended to create any private rights, privileges, benefits or causes of action in law or equity."[69] Thus, the *Guidelines* are not legally enforceable.

To date, the federal government and state governments have not adopted any legislation governing the video surveillance of public places.[70] In 2010, Senator Arlen Specter introduced a bill that would have placed some limits on lawful public video surveillance, but the bill never passed out of committee.[71] The bill itself would not have gone very far to address public privacy concerns resulting from video surveillance in public spaces. Rather, it focused on surveillance of an individual's place of residence—a location long understood by courts to enjoy a high level of Fourth Amendment protection.[72] The bill would simply have amended the federal criminal code "to prohibit unauthorized video surveillance of an individual in an area of a temporary or permanent residence that is not readily observable from a public location, with a reasonable expectation of privacy in the area."[73] It would also have generally prohibited the use of such surveillance as evidence.[74] The bill may yet come up for a vote: to date, it has been read twice in session and referred to the Committee on the Judiciary.[75]

Outside of legislation, while courts in the United States have addressed numerous surveillance issues,[76] they have not specifically addressed video surveillance in public areas. Local governments too have generally not regulated video surveillance programs. At least one survey has shown that most large police departments in the United States do not have written policies regulating the use of video systems.[77] This is pointed to by proponents of the NYPD's system, which has been applauded for voluntarily adopting a policy on privacy and abuse.[78] While New York City does have a policy, the policy as adopted provides no legally enforceable cause of action,[79] and the NYPD

69. *Id.* at 7.

70. Jeremy Brown, *Pan, Tilt, Zoom: Regulating the Use of Video Surveillance of Public Places*, 23 BERKELEY TECH. L.J. 755, 760 (2008) (citing Thomas D. Colbridge, *Electronic Surveillance: A Matter of Necessity*, FBI L. Enforcement Bull., Feb. 2000, at 26).

71. Surreptitious Video Surveillance Act of 2010, S. 3214, 111th Cong. (2010).

72. *See, e.g.*, Kyllo v. U.S., 533 U.S. 27 (2001) (acknowledging an individual's reasonable expectation of privacy at home).

73. S. 3214.

74. *Id.*

75. *Id.*

76. *See, e.g.*, Kyllo v. U.S., 533 U.S. 27 (2001); Dow Chemical Co. v. U.S., 476 U.S. 227 (1985); Katz v. U.S., 389 U.S. 347 (1967).

77. Thomas J. Nestel III, Using Surveillance Camera Systems to Monitor Public Domains: Can Abuse Be Prevented? 20 (March 2006) (unpublished M.A. thesis, Naval Postgraduate School), *available at* http://www.hsdl.org/?view&did=461595.

78. Anonymous Interview, *supra* note 9.

79. NYPD Guidelines, *supra* note 34, at 7.

has attempted to avoid making background information about that policy available to the public at large.[80]

### C. *Freedom of Information*

In 2007, the NYCLU filed Freedom of Information Law (FOIL)[81] and Freedom of Information Act (FOIA)[82] requests with the NYPD and the Department of Homeland Security (DHS), in an attempt to draw a picture for the public of how the City's video surveillance system is being implemented and operated.[83] The NYCLU sought the following information: the types of data the NYPD was planning to collect through the LMSI, how the data would be used, whether and how the data would be shared with other law enforcement agencies or other entities, the forms in which the data would be retained, and the length of time the data would be retained.[84] The NYPD initially responded to the NYCLU's request for documents by sending one document, and asserting that the rest of the documents sought "were either exempt from disclosure or could not be located."[85] Following an administrative appeal, eighty-eight additional documents were disclosed—mostly budgetary worksheets and funding requests.[86] The remaining undisclosed documents, by the NYPD's own calculations, totaled more than 2,100 pages and were found to be exempt from disclosure in the administrative appeal.[87]

---

80. *See* N.Y. Civil Liberties Union v. N.Y.C. Police Dep't, No. 112145/08, 2009 N.Y. Misc. LEXIS 2542 (N.Y. Sup. Ct. June 26, 2009).

81. N.Y. PUB. OFF. LAW § 84–90 (McKinney 2010).

82. Freedom of Information Act (FOIA), 5 U.S.C.A § 552 (West 2012).

83 *N.Y. Civil Liberties Union*, 2009 N.Y. Misc. LEXIS 2542; *see also* N.Y. Civil Liberties Union v. Dep't of Homeland Sec., 771 F. Supp. 2d 289 (S.D.N.Y. 2011) (No. 09-CV-5325).

84. *N.Y. Civil Liberties Union*, 2009 N.Y. Misc. LEXIS 2542 at *3.

85. *Id.*

86. *Id.* at *3–4.

87. *Id.* at *4–5. In the administrative hearing, the documents requested by the NYCLU were found to be exempt from disclosure under the following:

> N.Y. PUB. OFF. LAW § 87(2)(a) (McKinney 2010) (exempts from disclosure records whose disclosure is otherwise barred by state or federal statutes); N.Y. PUB. OFF. LAW § 87(2)(e)(i) (McKinney 2010) (exempts from disclosure records that are compiled for law enforcement purposes); N.Y. PUB. OFF. LAW § 87(2)(e)(iv) (McKinney 2010) (exempts records which, if disclosed, would interfere with law enforcement investigations or judicial proceedings, or reveal criminal investigative techniques or procedures, except routine techniques and procedures); N.Y. PUB. OFF. LAW § 87(2)(f) (McKinney 2010) (exempts from disclosure records whose disclosure could endanger the life or safety of a person); N.Y. PUB. OFF. LAW § 87(2)(g) (McKinney 2010) (exempts from disclosure inter-agency and intra-agency communications which are pre-decisional and deliberative); and, N.Y. PUB. OFF. LAW § 87(2)(i) (McKinney 2010) (exempts from disclosure records that, if disclosed, would jeopardize an agency's capacity to guarantee the security of its information technology assets, such assets encompassing both electronic information systems and infrastructures).

*Id.*

In 2008, the NYCLU sought judicial review of the NYPD's avoidance of the NYCLU's 2007 FOIL request for documents related to the LMSI.[88] In 2009, Justice Marylin Diamond of the New York State Supreme Court ordered the NYPD to disclose further documents, but upheld the exemption of any documents involving "the operational details of the LMSI, such as the types of information to be collected and how the information will be used, shared and stored and for how long" under Public Officers Law § 87(2)(e).[89] The court expressed concern that such disclosure would limit the effectiveness of the program and increase the risk of terrorist attacks in New York City.[90] The court responded to the NYCLU's request relating to funds received for the program and communications with vendors by ordering the production of documents for *in camera* review.[91]

On October 27, 2010, Justice Diamond filed a ruling.[92] With respect to documents classified as inter-agency and intra-agency communications, Justice Diamond ruled in favor of the NYPD, allowing such documents to be withheld from the NYCLU and, by extension, from the public.[93] The cumulative result of Justice Diamond's 2009 and 2010 rulings exempted from disclosure all documents that address operational details of the LMSI (such as the types of information to be collected, how such information will be used, shared and stored, and for how long), as well as any communications within and between agencies involved in the LMSI (which could include entities ranging from the NYPD to Goldman Sachs, a LMSI/MMSI stakeholder). With respect to all other documents, Justice Diamond did rule in favor of the NYCLU, ordering the NYPD to produce the requested documents.[94] To date, the NYPD has complied with the order, producing a series of documents that the NYCLU has been able to make use of in its advocacy work.[95] The NYCLU has had more success in retrieving documents from DHS in federal court, but, particularly in the absence of documents shedding light on the operation of LMSI/MMSI, or the communications between stakeholders in establishing the programs, the NYCLU has expressed continued concerns regarding the opacity in the management and operation of the LMSI and its progeny.[96]

---

88. *Id.* at *1.

89. *Id.* at *9–10.

90. *Id.* at *10.

91. *Id.* at *12.

92. N.Y. Civil Liberties Union v. N.Y.C. Police Dep't, No. 112145 (N.Y. App. Div. Oct. 27, 2010).

93. *Id.*

94. *Id.*

95. E-mail from Chris Dunn, Assoc. Legal Dir. of the N.Y. Civil Liberties Union, to author (Jan. 17, 2012, 1:44:29 PM EST) (on file with author).

96. N.Y. Civil Liberties Union v. N.Y.C. Police Dep't, 2009 N.Y. Misc. LEXIS 2542 at *12; *see also* Jen Chung, *NYCLU Wants Details on NYPD's Lower Manhattan Security Plans*, THE GOTHAMIST (Sept. 9, 2008, 5:33 PM), http://gothamist.com/2008/09/09/nyclu_wants_details_on_nypds_lower.php; Andrew Grossman, *With New Subway Cameras,*

### D. *A Comparison: Surveillance Law in the United Kingdom*

The United Kingdom has led the way in the adoption of video surveillance systems, and is cited often in relationship to emergent surveillance systems in the United States—notably, the LMSI/MMSI programs in New York City. As such, it is useful to consider the legal regime that regulates video surveillance in Britain, and to note that it does not differ substantially from our own legal regulation (and lack thereof) of video surveillance (although Parliament is in the process of considering a bill to increase civil liberties protections, which is discussed below).[97] A commonly cited statistic is that the United Kingdom deploys one surveillance camera for every fourteen citizens, and that the average citizen may be filmed up to 300 times per day; the United Kingdom is one of the top five most heavily surveilled countries in the world.[98] The Regulation of Investigatory Powers Act 2000 (RIPA),[99] the Police Act of 1997,[100] and the Intelligence Services Act of 1994 all compel the regulation of various surveillance methods in the United Kingdom.[101] This combination of statutes acts very much like the suite of federal legislation that governs surveillance in the United States: the PATRIOT Act,[102] the Electronic Communications Privacy Act,[103] the Communications Assistance for Law Enforcement Act,[104] and the Foreign Intelligence Surveillance Act.[105] On both sides of the Atlantic, these collections of legislation establish guidelines for surveillance activities, and generally provide the governments of the United States and the United Kingdom broad latitude in conducting surveillance of both citizens and noncitizens.

---

*an Attempt to Recreate "Ring of Steel" in Manhattan*, WALL ST. J. METROPOLIS BLOG (Sept. 20, 2010, 5:26 PM), http://blogs.wsj.com/metropolis/2010/09/20/with-new-subway-cameras-an-attempt-to-recreate-ring-of-steel-in-midtown.

97. Protection of Freedoms Bill, 2010-12, H.L. Bill [128] (Eng.) (introducing a code of practice for surveillance camera systems, among other provisions).

98. *Britain is "Surveillance Society*," BBC NEWS (Nov. 2, 2006), http://news.bbc.co.uk/2/hi/uk_news/6108496.stm; Tom Kelly, *Revealed: Big Brother Britain Has More CCTV Cameras than China*, DAILY MAIL (Aug. 11, 2009), http://www.dailymail.co.uk/news/article-1205607/Shock-figures-reveal-Britain-CCTV-camera-14-people--China.html; Sarah Lyall, *Britons Weary of Surveillance in Minor Cases*, N.Y. TIMES (Oct. 24, 2009), http://www.nytimes.com/2009/10/25/world/europe/25surveillance.html?pagewanted=all.

99. Regulation of Investigatory Powers Act, 2000, S.I. 2000/23 (U.K.).

100. Police Act, 1997, S.I. 1997/50 (U.K.).

101. Intelligence Services Act, 1994, S.I. 1994/13 (U.K.).

102. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Pub. L. No. 107-56, 115 Stat. 272 (2001) (codified in scattered titles and sections of U.S.C.).

103. The Electronic Communications Privacy Act of 1986 (ECPA), Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified at 18 U.S.C. §§ 2510–2522).

104. Communications Assistance for Law Enforcement Act (CALEA), Pub. L. No. 103-414, 47 U.S.C. §§ 1001–1010 (1994).

105. Foreign Intelligence Surveillance Act (FISA), Pub. L. No. 95-511, 92 Stat. 1783 (1978) (codified at 50 U.S.C. § 36).

Notably, the United Kingdom's legal framework on surveillance also resembles the law of the United States insofar as it lacks regulations that directly address public video surveillance. Parliament, however, is in the process of considering a bill aimed at "safeguard[ing] civil liberties and reduc[ing] the burden of government intrusion into the lives of individuals."[106] The Protection of Freedoms Bill was introduced into the House of Commons in February 2011, and according to the Home Office, is expected to complete the parliamentary process and receive Royal Assent by the end of the current session in April 2012.[107] As part of its provisions, the Bill would require the Secretary of State to promulgate a *Code of Practice* governing video surveillance and would establish a Surveillance Camera Commissioner, charged with "encouraging compliance with the surveillance camera code, reviewing the operation of the code, and providing advice about the code."[108] The *Code of Practice*, which will be adopted if Parliament passes the Protection of Freedoms Bill, resembles the NYPD's *Public Security Privacy Guidelines* in the privacy issues that it reaches (including technical specifications, retention of and access to data, and privacy training for personnel).[109] Unlike the *Guidelines*, however, the *Code of Practice* will be statutory and thus legally binding.[110]

While the *Code of Practice*, if implemented, will be legally binding, the Protection of Freedoms Bill sets out only vague and quite flexible provisions for the drafting of the code, and also has limited geographical and jurisdictional reach. The Bill does not mandate precisely what systems and uses must be addressed by the code. The code "must contain guidance about one or more of . . . the development or use of surveillance camera systems" or the "use or processing" of information obtained through those systems.[111] Additionally, regulations under the *Code of Practice* will govern only police and local governments, despite the fact that the use of video surveillance is more widespread.[112] Further, the draft document provided to the public for comment expresses a commitment to "restoring and preserving [the United Kingdom's] historic and valued traditions of freedom and fairness,"[113] but notes that "a cornerstone of a free and confident society is the State's duty to ensure that its citizens are sufficiently protected so that they are able to conduct their legitimate business in safety and security."[114] To

106. Protection of Freedoms Bill, 2010-12, H.L. Bill [128] (Eng.).
107. *Id.*
108. *Id.* cl. 29–38; *accord* S.A. Mathieson, *CCTV and ANPR to Get Commissioner and Code*, The Guardian (Feb. 11, 2011), http://www.guardian.co.uk/government-computing-network/2011/feb/11/cctv-commissioner-code-anpr-freedoms-bill.
109. Protection of Freedoms Bill, 2010-12, H.L. Bill [128] cl. 29(3) (Eng.).
110. *Id.* cl. 29(1).
111. *Id.* cl. 29(2).
112. *Id.* cl. 33(5); Mathieson, *supra* note 108.
113. *Id.* at 3.
114. *Id.*

that end, the Code asserts that nothing in it is intended to "hamper the ability of the law enforcement agencies or any other organisation, to use [video surveillance technology] as necessary to prevent or detect crime, or otherwise help to ensure the safety and security of individuals."[115] Much like the NYPD's *Guidelines*, the Code of Practice aims to ensure the utmost flexibility to agencies engaging in video surveillance. Finally, of concern to critics of the Bill is the fact that individuals who fail to follow the code will face neither civil nor criminal charges.[116]

As in the United States, the authority of British national, regional, and local governments to conduct any type of surveillance is subject to a "reasonable expectation of privacy" standard.[117] The definition of a reasonable expectation of privacy anywhere except in the home remains as uncertain in the United Kingdom as it does in the United States.[118] A key difference between the laws of the United Kingdom and the United States, however, is that the reasonable expectation of privacy standard in the United Kingdom does not stem from national law; rather, it comes from the European Convention on Human Rights (ECHR), to which the United Kingdom is subject, along with the rest of the European Union.[119] Article 8 of the ECHR provides that "everyone has the right to respect for his private and family life, his home and his correspondence" and prohibits government interference with this right,

> except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of

115. *Id.*

116. Protection of Freedoms Bill, 2010-12, H.L. Bill [128] cl. 33(2) (Eng.); Mathieson, *supra* note 108.

117. Peck v. U.K., 2003-I Eur. Ct. H.R. 57; Monica Bhogal, *United Kingdom Privacy Update 2003*, 1 SCRIPT-ED 205, 211 (2004), *available at* http://www.law.ed.ac.uk/ahrc/script-ed/docs/privacy.pdf; Clare Feikert & Charles Doyle, *Anti-Terrorism Authority Under the Laws of the United Kingdom and the United States*, FED'N OF AM. SCIENTISTS 17 (Sep. 7, 2006), *available at* www.fas.org/sgp/crs/intel/RL33726.pdf.

118. In the United Kingdom, see THE ROYAL ACAD. OF ENG'G, DILEMMAS OF PRIVACY AND SURVEILLANCE CHALLENGES OF TECHNOLOGICAL CHANGE 32 (2007), *available at* http://www.raeng.org.uk/news/publications/list/reports/dilemmas_of_privacy_and_surveillance_report.pdf ("There is need for clarification of the notion of a 'reasonable expectation of privacy' in order that the right to privacy is better understood and better protected."). In the United States, there is no reasonable expectation of privacy in information "knowingly exposed" to a third party, but while certain data has been established as knowingly exposed, the full spectrum of privacy from knowing exposure to reasonable expectation of privacy is not clearly defined. *See, e.g.*, Kyllo v. U.S., 533 U.S. 27 (2001) (acknowledging an individual's reasonable expectation of privacy at home); Smith v. Maryland, 442 U.S. 735 (1979) (holding that the installation and use of a "pen register" is not a search within the meaning of the Fourth Amendment); U.S. v. Miller, 425 U.S. 435 (1976) (holding that the Fourth Amendment does not protect bank account information divulged to banks by account holders).

119. Feikert, *supra* note 117, at 14.

> disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[120]

While Article 8 leaves room for a wide range of government actions in the interest of security and safety, to date the European Court of Human Rights has construed the article somewhat protectively in favor of individual privacy rights.[121]

In Europe, there appears to be more room than in the United States for protections against privacy violations that occur in public. The European Court of Human Rights has identified a "zone of interaction of a person with others, even in a public context, which may fall within the scope of 'private life.' "[122] In the 2003 case *Peck v. The United Kingdom*,[123] for example, the Court firmly expressed the principle that, under certain circumstances, an individual's actions in a public place may retain a reasonable expectation of privacy, despite taking place in public.[124] In *Peck*, the claimant was filmed on a surveillance camera and still images from the surveillance footage were later released to the media. Peck's application for judicial review in the United Kingdom was rejected on the grounds that there was no general right of privacy under English law.[125] Peck then brought his claim to the European Court of Human Rights, which ruled that the disclosure of footage constituted a disproportionate interference with Peck's private life—a term construed broadly under Article 8 of the ECHR—and the fact that the footage was taken on a public street was not sufficient to preclude it from being considered a private situation.[126] The *Peck* ruling and others like it are significantly different from the jurisprudence of the United States, which, to date, has found no reasonable expectation of privacy in public under any circumstances.[127]

In practice, the construction of privacy rights by the European Court of Human Rights may not grant substantially greater privacy protections to the average British citizen than is afforded to the average American citizen. *Peck* is a substantially limited ruling, based on unique circumstances involving a highly mentally-disturbed claimant on the street at night, with a privacy claim based not on the government's act of filming him, but rather on its subsequent act of releasing stills from the footage. Further, any

---

120. The European Convention on Human Rights, art. 8, Nov. 4, 1950, C.E.T.S. No. 5.

121. Bhogal, *supra* note 117.

122. P.G. and J.H. v. U.K., 2001-IX Eur. Ct. H.R. 56–57.

123. Peck v. U.K., 2003-I Eur. Ct. H.R. 57.

124. *Id.* at §§ 62, 63.

125. *Id.* at § 32 (citing the High Court of England and Wales, which noted that there is no general right of privacy recognized by English law).

126. *Id.* §§ 62, 63, 85.

127. U.S. v. Knotts, 460 U.S. 276, 281 (1983) ("A person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."); Katz v. U.S., 389 U.S. 347, 351 (1967) ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.").

individual wishing to challenge the government's video surveillance practices can rely only on the ECHR and litigation in the European Court of Human Rights. Just as an American citizen must have resources and stamina to bring an individual privacy claim, so too must a British citizen summon the same wherewithal to bring a claim to the European Court of Human Rights. While the European law may prove to be somewhat more protective of individual privacy rights, the path to judicial review may not be more readily available than the path to judicial review in the United States.

## III. Security versus Privacy and Free Speech

### A. *Painting a Picture*

The NYCLU demanded documents from the NYPD to develop a picture of the policies in place (or lack thereof) governing New York City's video surveillance programs, so as to be able to effectively monitor and respond to potential abuses and violations of the system.[128] The lack of legally enforceable guidelines and/or any governing legislation raises major concerns having to do with privacy protections, as well as First Amendment rights. Some of these privacy concerns relate to the length of time that the NYPD may keep footage from the video surveillance system and regulations regarding how and under what circumstances such footage may be shared between departments, between stakeholders, and even between state and federal law enforcement entities. Further concerns deal with basic privacy issues—how far into individuals' lives video cameras may probe—and the possible chilling effect of such surveillance upon New Yorkers' speech. The *Guidelines* set out a range of operational procedures. However, with no possibility of legal enforcement, these procedures do not provide strong protections against law enforcement overstepping its bounds.

There is no obvious legal argument to challenge the omnipresence and expansion of surveillance cameras in New York City. As Chris Dunn, Associate Legal Director of the NYCLU, puts it, "I know of no plans by any organization to litigate the presence of surveillance cameras in New York, and you can read into that the absence of a good legal argument against them."[129] There has been no domestic litigation regarding the overarching legality of public video surveillance.[130] The lack of such litigation seems to reflect and affirm the view that systems such as the LMSI/MMSI cannot be facially challenged. That is, the system, on its face, does not violate the United States Constitution, nor does it violate any federal or state statute. Any challenge would have to be to a specific application of the system—a

128. Dunn Interview, *supra* note 12, at 1.
129. *Id.*
130. *Id.*

specific instance of overreach or abuse.[131] However, in other contexts courts have acted to place certain limits on the reach of different types of surveillance, and these limitations help illustrate where boundaries and possible overreaching may be identifiable with regard to video surveillance, laying groundwork for possible legal challenges to particular practices.

Any potential legal arguments challenging public video surveillance programs would have to be grounded primarily in the Fourth Amendment,[132] and potentially in the First Amendment as well.[133] With regard to the Fourth Amendment, there are three notable, relevant boundaries that the judiciary has placed on surveillance practices through case law, offering some guidance as to the limits of constitutional video surveillance.[134] First, public video surveillance cameras may not be used to monitor spaces in which individuals have a reasonable expectation of privacy.[135] Second, police may not use zoom lenses to magnify individuals, belongings, or activity to an invasive degree without a warrant.[136] Third, police may not use cameras to conduct extensive surveillance without suspicion.[137] While these three guidelines are broad, and in some cases come from Supreme Court dicta, they at least set out possible boundaries to consider in the absence of clear standards. The First Amendment may provide additional support for a challenge. Constitutional concerns would relate to the potential chilling effect on freedom of speech and association that could result from surveillance practices.

---

131. The Supreme Court, in considering constitutional challenges to legislation, distinguishes between facial challenges, which assert that "no set of circumstances exists under which the Act [in question] would be valid," U.S. v. Salerno, 481 U.S. 739, 745 (1987), and "as applied" challenges, which challenge the validity of legislation only as applied to the challenger's particular actions or circumstances, Ohralik v. Ohio State Bar Ass'n, 436 U.S. 447, 462 (1978).

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

133. 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.").

134. Brown, *supra* note 70, at 767.

135. *See* Katz v. U.S., 389 U.S. 347, 351 (1967) (holding that the Fourth Amendment protects individuals who have an expectation of privacy that is recognized as reasonable by society).

136. *See* Dow Chem. Co. v. U.S., 476 U.S. 227, 238 n.5 (1985) (suggesting that zooming in with a video camera to a certain point might become so invasive as to require a warrant).

137. *See* U.S. v. Knotts, 460 U.S. 276, 283–84 (1983) (finding that a radio transmitter attached to defendant's property that indicated defendant's location to law enforcement officers did not constitute an unlawful search within the meaning of the Fourth Amendment, but suggesting that systems that make possible "twenty-four hour surveillance of any citizen" and "dragnet-type law enforcement practices" could potentially raise Fourth Amendment concerns).

### B. *Video Abuse*

New York City history reveals prevalent opportunities for abusive practices in video surveillance, including violations of privacy, chilling of free speech, and discrimination. The fact that the NYPD's *Guidelines* are not legally enforceable, combined with the lack of any official acknowledgement of—or commitment to move away from—past practices, strengthens civil liberties advocates' view that abusive practices are likely to be repeated, and will go unnoticed and unchallenged in many cases.[138]

New York City's history of abusive surveillance practices dramatically highlights the importance of public knowledge of video surveillance programs and the guidelines surrounding their implementation and use by the NYPD. The abuses made possible by video surveillance may seem obvious and unnecessarily re-hashed here. But it is important to take into account the human impact of such incidents, to make the consequences tangible. As Chris Dunn explains, until the public has a clear understanding of the privacy threat imposed by video surveillance, there is little possibility that more stringent regulations will materialize.[139]

The NYPD emphasizes a distinction between its anti-crime surveillance programs and its Counterterrorism Bureau's LMSI/MMSI program, implying that the Counterterrorism Bureau's program is better monitored and more tightly controlled to prevent abuses.[140] That the *Guidelines* were voluntarily adopted has been promoted as evidence of the NYPD's recognition of the "magnitude" of the new surveillance programs, and its commitment to "respecting" the public's privacy concerns.[141] The NYPD also admittedly anticipated challenges to the system and aimed to create, in the *Guidelines*, a framework for "the responsible use of such a system."[142] However, as much as we may wish to ascribe only good will and good faith to our law enforcement officers, the reality is that they may make mistakes.

A National Institute of Justice study shows that law enforcement officers can have trouble concentrating on surveillance monitors after they have

---

138. *See generally* WHO'S WATCHING?, *supra* note 15 (asserting that New York City's video surveillance activities, and the lack of legally enforceable regulations of those activities, create a law enforcement climate in which abuses will be replicated, and that without legal checks to the system, many abuses will go unnoticed and unaddressed, because individuals will not be sufficiently informed or empowered to challenge them).

139. Dunn Interview, *supra* note 12, at 1.

140. Anonymous Interview, *supra* note 9 (noting that all personnel in the coordination center are required to take a three-hour privacy training course that the NYPD developed specifically for using the Domain Awareness System); *see also* NYPD Guidelines, *supra* note 34, at 6–7 (providing that all stakeholder representatives and NYPD personnel are required to complete a privacy training "based, in part, upon a curriculum covering the proper use and handling of such information, with periodic assessments").

141. Anonymous Interview, *supra* note 9.

142. *Id.*

been watching for more than twenty minutes,[143] resulting in possible slips in diligence, or unethical actions born of boredom. Even assuming nothing but good intentions on the part of New York City police officers, there can be no mistaking the fact that incidents of abuse can and do occur. LMSI/MMSI is run out of the same police department as anti-crime surveillance programs, and is staffed primarily by New York City police officers.[144] It is therefore reasonable to use VIPER and other related programs as at least an illustration of some of the possible consequences of police video surveillance programs in New York City.

### 1. Privacy

During the 2004 Republican National Convention in New York, a NYPD helicopter, equipped with an infrared camera, was tasked with monitoring a mass bicycle ride protest through downtown Manhattan.[145] During the course of their duties, the police officers controlling the helicopter also recorded a couple being intimate on an apartment terrace, for nearly four minutes.[146] The recording became public when it was used in the trial of one of the protesting bikers, and it was eventually aired by the local CBS station.[147] Jeffrey Rosner, one of the filmed individuals, said following the incident (and after filing a complaint) that he tended to be in favor of surveillance, but that he was concerned with "the sensibility that the police think it's O.K. that they do that—it's about their own professionalism."[148]

In addition to such a remarkable incident, the use of surveillance cameras has everyday privacy implications. Many of the cameras in New York City, especially prior to the LMSI/MMSI programs, have been set up to be un-manned, static monitors, which can be referred back to in case of an incident. Others, however, even prior to LMSI/MMSI, have been run and monitored in real time by police officers, leaving these cameras to be especially potent potential tools of misuse. As reported by the *Associated Press*,

---

143. The National Institute of Justice has reported on experiments that were run "to test the effectiveness of an individual whose task was to sit in front of a video monitor(s) for several hours a day and watch for particular events. These studies demonstrated that such a task, even when assigned to a person who is dedicated and well-intentioned, will not support an effective security system. After only twenty minutes of watching and evaluating monitor screens, the attention of most individuals has degenerated to well below acceptable levels." MARY W. GREEN, NAT'L INST. OF JUSTICE, THE APPROPRIATE AND EFFECTIVE USE OF SECURITY TECHNOLOGIES IN U.S. SCHOOLS: A GUIDE FOR SCHOOLS AND LAW ENFORCEMENT AGENCIES, 30 (1999), *available at* https://www.ncjrs.gov/school/home.html.

144. Anonymous Interview, *supra* note 9; NYPD Press Release, *supra* note 8.

145. Jim Dwyer, *Police Video Caught a Couple's Intimate Moment on a Manhattan Rooftop*, N.Y. TIMES, Dec. 22, 2005, at B10; *NYCLU Decries NYPD Abuse of Infrared Cameras During RNC*, N.Y. CIV. LIBERTIES UNION (Feb. 24, 2005), http://www.nyclu.org/news/nyclu-decries-nypd-abuse-of-infrared-cameras-during-rnc.

146. Dwyer, *supra* note 145, at B10.

147. *Id.*

148. *Id.*

police officers have regularly used video surveillance cameras to engage in "up-skirting" and "down-blousing"—using cameras to take pictures up women's skirts or down their blouses on city streets.[149] Former New York City Councilman and New York State Senator Hiram Monserrate, a retired police officer, publicly recalled behavior he observed while part of a Queens VIPER unit: "Some of the stuff I witnessed was what I would term as clearly inappropriate use of the cameras in their surveillance—whether they are looking into people's windows or some of the male police officers looking at women."[150]

Studies show that the majority of Americans feel, as Jeffrey Rosner does, that video surveillance is warranted, and applaud its use to keep us safe.[151] However, any argument for video surveillance based on security needs must take into account the reality that individuals make unwise, unethical, and privacy-violating choices with some regularity. Without enforceable regulations, disclosure, and public conversation, such incidents will largely go unacknowledged and unaddressed. As Jeffrey Brown points out, "In the way that the digital revolution has allowed consumers to easily distribute, download, and edit movies and songs, it has allowed police to do the same with surveillance footage."[152] Unchecked, these systems offer too much potential, and even temptation, for abusive practices.

### 2. Free Speech

Another concern posed by video surveillance is the potential for infringement on freedom of speech and association.[153] The ACLU of Northern California (ACLU-NC) has taken the position that video cameras in public may chill speech by preventing anonymity.[154] It has long been established by the Supreme Court that it is unconstitutional for the government to require

149. WHO'S WATCHING?, *supra* note 15, at 12 (citing *Three Arrested After Traffic Camera Aimed at Passerby*, ASSOCIATED PRESS (Sept. 15, 2003), *available at* http://www.notbored.org/camera-abuses.html).

150. *Id.* (citing Sarah Wallace, *Exclusive: NYPD Housing Surveillance Staffed By Cops Under Investigation*, WABC N.Y. (Apr. 22, 2004), transcript *available at* http://nyc.indymedia.org/en/2004/04/37792.html).

151. *See, e.g.*, John Esterbrook, *Poll: Americans OK With Video Scrutiny*, CBS NEWS (Feb. 11, 2009), *available at* http://www.cbsnews.com/stories/2002/04/21/opinion/polls/main506822.shtml (stating that Americans are willing to "put up with" surveillance cameras in public places and "feel, by a three-to-one margin (72%–24%), that they will have to give up some of their personal freedoms in order to make the country safe from terrorist attacks"); *see also* Dwyer, *supra* note 145, at B10.

152. Brown, *supra* note 70, at 762.

153. MARK SCHLOSBERG & NICOLE A. OZER, AM. CIVIL LIBERTIES UNION OF NORTHERN CAL., UNDER THE WATCHFUL EYE: THE PROLIFERATION OF VIDEO SURVEILLANCE SYSTEMS IN CALIFORNIA 7 (2007), *available at* http://www.aclunc.org/docs/criminal_justice/police_practices/under_the_watchful_eye_the_proliferation_of_video_surveillance_systems_in_california.pdf [hereinafter UNDER THE WATCHFUL EYE].

154. *Id.*

individuals to identify themselves while speaking in public,[155] or to require the disclosure of membership lists.[156] The ACLU-NC argues that "[i]nstalling cameras in public spaces is tantamount to requiring people to identify themselves whenever they walk, speak, or meet in public."[157] It is widely accepted that surveillance practices may have a "chilling effect" on individuals' freedom of expression and association.[158] The ACLU-NC argues that a video camera trained on the entrance of a building where an organization holds meetings could reveal that organization's members just as easily as a disclosed membership list.[159] In *NAACP v. Alabama*, the constitutional violation at issue was the state's attempt to force the NAACP to disclose its membership list.[160] The use of video surveillance to videotape the entryway to an organization's place of business or meeting location, however, might enable a government to surreptitiously obtain the equivalent of a membership list without having to make a request and without providing notice to the organization or its members. Fear of identification, as the Supreme Court noted in *NAACP v. Alabama*, can chill speech by discouraging membership in various types of organizations, the sharing of viewpoints at odds with the government, or even simply being seen in certain places.[161] These, in fact, have been the results of past NYPD surveillance efforts in New York City.

New York City has a long history of police surveillance of individuals and groups engaged in political protest and dissent.[162] Between 1904 and

155. *See* Buckley v. Am. Constitutional Law Found., 525 U.S. 182 (1992) (holding that Colorado could not require petition solicitors to wear identification badges because such a requirement "discourages participation in the petition circulation process by forcing name identification without sufficient cause").

156. NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449 (1958) (holding that the state of Alabama could not compel the NAACP to disclose its membership lists).

157. *Id.*

158. *See, e.g.*, Buckley v. Valeo, 424 U.S. 1, 64 (1976) ("[C]ompelled disclosure . . . can seriously infringe on privacy of association and belief guaranteed by the First Amendment"); *NAACP*, 357 U.S. at 462 ("This Court has recognized the vital relationship between freedom to associate and privacy in one's associations. . . . Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association."); Am. Civil Liberties Union, *What's Wrong With Public Video Surveillance?* (Feb. 25, 2002), http://www.aclu.org/technology-and-liberty/whats-wrong-public-video-surveillance; Jessica Pupovac, *Chill of Govt. Surveillance Grips Activists, Muslims*, THE NEW STANDARD (Jul. 11, 2006), http://www.truth-out.org/article/chill-government-surveillance-grips-activists-muslims; Teresa Watanabe and Paloma Esquivel, *L.A. Area Muslims Say FBI Surveillance Has a Chilling Effect on Their Free Speech and Religious Practices*, L.A. TIMES (Mar. 1, 2009), http://articles.latimes.com/2009/mar/01/local/me-muslim1; *see also* Matthew Taylor and Paul Lewis, *Surveillance of Arms Trade Campaigner Was Unlawful, Says Appeals Court*, THE GUARDIAN (May 21, 2009), http://www.guardian.co.uk/uk/2009/may/21/campaigner-police-surveillance-ruled-unlawful.

159. UNDER THE WATCHFUL EYE, *supra* note 153, at 7.

160. *NAACP*, 357 U.S. at 449.

161. *NAACP*, 357 U.S. at 462.

162. *See* WHO'S WATCHING, *supra* note 15; Dunn Interview, *supra* note 12.

1985 the NYPD compiled intelligence files on more than 200,000 individuals and groups, including those who were suspected of being communists, Vietnam War protesters, health and housing advocates, education reform groups, and civil rights activists.[163] In 1985, a class-action lawsuit finally led to limitations on the NYPD's surveillance activities.[164] The resulting "Handschu Agreement" prohibited the NYPD from investigating the political, ideological or religious activities of an individual or group unless the department had "specific information . . . that a person or group engaged in political activity is engaged in, about to engage in or has threatened to engage in conduct which constitutes a crime."[165] However, in 2003, largely as a result of concerns about terrorism in the wake of September 11th, the United States District Court for the Southern District of New York modified the Handschu Agreement, allowing the NYPD far greater latitude to monitor individuals involved in political activity.[166] Under the new guidelines, the police may commence a preliminary inquiry based upon "information indicating the *possibility* of unlawful activity."[167]

The result of the relaxation of the Handschu Agreement was evident during the 2004 Republican National Convention. Without notice to the public, the NYPD deployed extraordinary numbers of surveillance cameras around the city (not only near Madison Square Garden, where the Convention was held),[168] and deployed police officers with hand-held cameras to videotape protesters.[169] Police intelligence officers were also deployed nationally and internationally, in advance of the Convention, to obtain information about individuals planning to visit New York City during the Convention—logging data about even those individuals with "no apparent intention of breaking the law."[170] Surveillance of this nature by the police comes remarkably close to the type of surveillance and data collection practiced by the NYPD in the decades prior to the Handschu Agreement. Human sensitivities to being monitored have not changed, and it remains likely that such activity by law enforcement agencies will lead to a chilling effect on speech and association.

---

163. Chisun Lee, *The NYPD Wants to Watch You*, VILLAGE VOICE (Dec. 17, 2002), http://www.villagevoice.com/2002-12-17/news/the-nypd-wants-to-watch-you/1; *see also* WHO'S WATCHING?, *supra* note 15, at 8.

164. Handschu v. Special Servs. Div., 605 F. Supp. 1384 (S.D.N.Y. 1985), *aff'd*, 787 F.2d 828 (2d Cir. 1986).

165. WHO'S WATCHING?, *supra* note 15, at 8; *see Handschu*, 605 F. Supp. at 1421.

166. *Handschu*, 288 F. Supp. 2d ("Second Revised Order and Judgment").

167. *Id.* at 422 (emphasis added); *see also* WHO'S WATCHING?, *supra* note 15, at 8–9.

168. WHO'S WATCHING?, *supra* note 15, at 9.

169. *Id.*; NEAL FEIGENSON & CHRISTINA SPIESEL, LAW ON DISPLAY: THE DIGITAL TRANSFORMATION OF LEGAL PERSUASION AND JUDGMENT 50 (2009) (noting that during the 2004 Republican National Convention uniformed and undercover police officers used small, handheld cameras to film as they moved through crowds).

170. Jim Dwyer, *City Police Spied Broadly Before G.O.P. Convention*, N.Y. TIMES (Mar. 25, 2007), http://www.nytimes.com/2007/03/25/nyregion/25infiltrate.html?pagewanted=all.

### 3. Discrimination and Bias

Discrimination and bias play an independent role in generating concerns about video surveillance, and they also heighten privacy infringement concerns and First Amendment chilling effects. While it is certainly not the intent of this Note to make a generalized accusation that New York City police officers are biased, the targeting of minority communities in New York City by the NYPD is long-standing. In 1999, then-Attorney General Eliot Spitzer issued a report that found that police officers in New York City disproportionately stopped and frisked blacks and Latinos as compared to whites.[171] A decade later, this trend was reaffirmed by a study conducted by Jeffrey A. Fagan.[172] The study showed not only continuing racial bias, but also data indicating that, in more than thirty percent of stops over the six years of the study, officers either lacked, or failed to report, the necessary suspicion to make a stop constitutional.[173]

The kind of active bias—whether conscious or unconscious—that is found in the NYPD's stop-and-frisk programs has also found its way into police video surveillance. In 2004, the general public was largely unaware of the NYPD's VIPER program. That changed when 22-year-old Paris Lane committed suicide in the lobby of the Morris Houses in the Bronx, and his death was caught on a surveillance camera monitored by VIPER Unit officers.[174] The video found its way onto *Consumption Junction*, an Internet site offering images of pornography and violence.[175] The video of Lane's death was labeled "Introducing: The Self-Cleansing Housing Project."[176] To add insult to injury, the video also made its way to Lane's foster mother, Martha Williams, who approached then-Manhattan Borough President C. Virginia Fields for help in holding the NYPD accountable for the sharing of the video.[177] The NYPD acknowledged that the camera that captured the suicide

171. Office of the N.Y. State Attorney Gen. Eliot Spitzer, The New York City Police Department's 'Stop-and-Frisk' Practices: A Report to the People of the State of New York 89 (1999), *available at* http://www.nysl.nysed.gov/scandoclinks/ocm43937374.htm ("There is a strong statistical correlation between race and likelihood of being 'stopped.' "); *see also* Guirguis, *supra* note 6, at 151 (noting that in 2000, the NYPD came under federal and state investigations for systematically targeting minorities in unwarranted traffic stops).

172. Al Baker & Ray Rivera, *Study Finds Street Stops by N.Y. Police Unjustified*, N.Y. Times (Oct. 26, 2010), http://www.nytimes.com/2010/10/27/nyregion/27frisk.html?_r=1&emc=eta1.

173. *Id.*

174. Who's Watching?, supra note 15, at 11.

175. *Id.*; Shaila K. Dewan, *Video of Suicide in Bronx Appears on Shock Web Site*, N.Y. Times (Apr. 1, 2004), http://www.nytimes.com/2004/04/01/nyregion/video-of-suicide-in-bronx-appears-on-shock-web-site.html; *Video of Suicide in Bronx Housing Project Turns Up on Website*, NY 1 News (Mar. 31, 2004), http://www.ny1.com/content/top_stories/38580/video-of-suicide-in-bronx-housing-project-turns-up-on-website.

176. Dewan, *supra* note 175.

177. *Id.*

recorded digital images, which meant that they could have been easily emailed.[178]

Williams' complaint led to a public hearing, and a series of formal questions posed to Police Commissioner Raymond Kelly by C. Virginia Fields.[179] Commissioner Kelly responded with assurances that the NYPD had regulations in place to protect tenants' privacy, VIPER Unit officers were trained and supervised, and videotapes were stored in secure locations and destroyed or erased after fourteen days unless they were needed for a criminal investigation.[180] However, interviews conducted by a reporter for *Eyewitness News* revealed a very different story. Former and current VIPER Unit officers shared stories of officers videotaping "residents of the housing development having sex" and sharing those videos with fellow officers.[181] They also clarified the discrimination that seems practically inherent in the program. As a former investigator stated, "If this was the Upper East Side it wouldn't be happening. No one would have cameras on. But because it's the so-called projects, no one really cares and it doesn't matter. We can film you, and have entertainment, and do what we want and no one cares."[182] It is difficult to imagine that incidents such as those that have occurred under VIPER and other NYPD programs would not be equally possible under LMSI/MMSI, particularly without implementation guidelines that are legally enforceable.

Finally, though it has not yet surfaced publicly in the United States, bias in video surveillance that targets Muslim citizens could very easily become a significant issue. In 2010, the British police apologized for having installed surveillance cameras, with no public notice, in predominantly Muslim areas of the city of Birmingham.[183] More than 200 cameras were placed in two Muslim neighborhoods in response to general concerns about Islamic fundamentalism and potential terrorism threats.[184] Recently, New York City has seen the implementation of an alleged secret NYPD surveillance program targeting Muslim communities,[185] and the revelation that at

178. WHO'S WATCHING?, *supra* note 15, at 11; Jen Chung, *Website's Suicide Video Seems to Lead Back to NYPD*, GOTHAMIST (Apr. 1, 2004), http://gothamist.com/2004/04/01/websites_suicide_video_seems_to_lead_back_to_nypd.php.

179. WHO'S WATCHING?, *supra* note 15, at 11.

180. *Id.* (citing letter from Raymond W. Kelly to C. Virginia Fields, Apr. 27, 2004, on file with the ACLU).

181. *Id.*; Sarah Wallace, *Exclusive: NYPD Housing Surveillance Staffed By Cops Under Investigation*, WABC NEW YORK (Apr. 22, 2004), *available at* http://nyc.indymedia.org/en/2004/04/37792.html.

182. WHO'S WATCHING?, *supra* note 15, at 11.

183. *British Police Offer Apology to Muslims for Spy Cameras*, N.Y. TIMES, Oct. 1, 2010, at A11.

184. *Id.*

185. New York City Council Public Safety Committee on NYPD Surveillance of Muslim New Yorkers (Oct. 6, 2011), *available at* http://www.nyclu.org/files/releases/Testimony_NYPD_Muslim_surveillance_10.6.11.pdf (testimony of Udi Offerson on behalf of the N.Y. Civil Liberties Union); *see Court Filing Seeks Information on NYPD Surveillance*

least 1,400 City police officers were shown a film during their training that characterized Muslims as seeking to "infiltrate and dominate" the United States.[186] New York City appears to be ripe for a similar scenario as Islamophobia grows across the United States.

## IV. Projections and Applications

Civil liberties advocates are most concerned by the lack of disclosure of how New York City's LMSI/MMSI video surveillance program operates and the absence of any legal cause of action for abuse under the program, both of which make the potential for violations far too great.[187] As the stories of Paris Lane and Jeffrey Rosner demonstrate, abuse of video surveillance systems happens, and there is no clear way of monitoring or preventing it. It is crucial that legally enforceable regulations be implemented to monitor and limit police and government use of video surveillance systems. Regulations should come from all levels of government, but most importantly at the local level, where city councils can address the security issues specific to their areas and balance the concerns of their constituents.

In New York City, two enormous barriers to discussion, debate, and enforcement of video surveillance regulations are the NYPD's court-supported refusal to release the majority of documents related to the operations of video surveillance programs and the unenforceable nature of the NYPD's *Public Security Privacy Guidelines*. To date, there has not been a single public hearing on LMSI/MMSI and their future progeny, nor has the City Council taken on the task of regulating them.[188] Without such efforts at public education, discussion, and regulation, as new technologies continue to develop the public will not have the opportunity to register concerns or advocate for building enforceable limits. This opens the way for future unfettered public surveillance.

---

*Targeting Muslims*, N.Y. Civ. Liberties Union (Oct. 3, 2011), http://www.nyclu.org/news/court-filing-seeks-information-nypd-surveillance-targeting-muslims; Colby Hamilton, *NYCLU Goes to Court Over NYPD's Muslim Surveillance*, WNYC The Empire (Oct. 3. 2011), http://empire.wnyc.org/tag/handschu; Colby Hamilton, *With CIA Help, NYPD Moves Covertly in Muslim Areas*, WNYC The Empire (Aug. 24, 2011), http://empire.wnyc.org/2011/08/ap-with-cia-help-nypd-moves-covertly-in-muslim-areas.

186. Michael Powell, *In Shift, Police Say Leader Helped with Anti-Islam Film and Now Regrets It*, N.Y. Times (Jan. 24, 2012), http://www.nytimes.com/2012/01/25/nyregion/police-commissioner-kelly-helped-with-anti-islam-film-and-regrets-it.html; *see also* Michael Powell, *In Police Training, A Dark Film on U.S. Muslims*, N.Y. Times (Jan. 23, 2012), http://www.nytimes.com/2012/01/24/nyregion/in-police-training-a-dark-film-on-us-muslims.html?_r=1&ref=nyregion.

187. Dunn Interview, supra note 12, at 1.

188. Letter from Christopher Dunn, Donna Lieberman, and Robert Perry, N.Y. Civil Liberties Union, to Comm'r Kelly and Deputy Comm'r Falkenrath, New York City Police Dep't (Mar. 26, 2009) 1, 3 (on file with the N.Y. Civil Liberties Union) (noting the lack of public hearings on the Lower Manhattan Security Initiative and the Public Security Privacy Guidelines, and calling for a formal, public review) [hereinafter Dunn Letter].

### A. *Mission Creep and Technological Advances*

Surveillance programs in New York City also contain strong potential for mission creep—the expansion of a project or a mission beyond its stated goals.[189] Law enforcement officers might use images for un-sanctioned or illegal purposes, such as to create video archives of protesters, or to target minority individuals.[190] Additional concerns include the lack of a legally cognizable, reasonable expectation of privacy on public streets, and the un-tested nature of applying the plain view doctrine (which allows law enforcement to seize, without a warrant, evidence found in plain view during a lawful observation)[191] to surveillance as technologies change. Individuals on the street are generally not protected by any reasonable expectation of privacy, with regard to actions or items that can be easily seen by normal vision.[192] While New Yorkers may not have a reasonable expectation of privacy on the street, it is not necessarily the case that we shed our privacy "in its entirety at [our] doorstep."[193] The problem is that we lack any real clarity as to the breadth of our privacy that remains once we leave our homes, as well as how a *reasonable* expectation of privacy is determined. From how far away may a camera zoom in on a letter we are reading on a park bench or an email on a Blackberry while walking—something likely unreadable by a police officer passing by? May a surveillance camera affixed to a lamppost record an intimate conversation on the other end of the block? May a camera peer through a car window?

Public video surveillance programs also have implications for at-home privacy. The Supreme Court's ruling in *Kyllo v. United States* established that Fourth Amendment protections are strongest in the home.[194] But the home is not sacrosanct. The Court preserved the "lawfulness of warrantless visual surveillance of a home,"[195] noting that, under the plain view doctrine, visual observation is not a search.[196] Without any clear limitations on video surveillance programs, it seems possible—if not likely—that the limits to Fourth Amendment protections in the home, affirmed by the Supreme Court in *Kyllo*, could make new types of privacy encroachments possible. One can imagine a surveillance camera with pan-tilt-zoom capabilities, affixed to a

189. *Mission Creep*, Merriam-Webster Online Dictionary, http://www.merriam-webster.com/dictionary/mission%20creep (last visited Mar. 23, 2012) (Mission creep is "the gradual broadening of the original objectives of a mission or organization.").

190. WHO'S WATCHING?, *supra* note 15, at 8.

191. *See, e.g.*, Ill. v. Andreas, 463 U.S. 765, 771 (1983) (explaining that the plain view doctrine is premised on the idea that when police are "lawfully in a position to observe an item firsthand, its owner's privacy interest in that item is lost").

192. Guirguis, *supra* note 6, at 157; *see also* Cal. v. Greenwood, 486 U.S. 35, 41 (1988); Ill. v. Andreas, 463 U.S. 765, 771 (1983).

193. Guirguis, *supra* note 6, at 157–58.

194. Kyllo v. U.S., 533 U.S. 27 (2001).

195. *Id.* at 27, 32.

196. *Id.*

public lamp post; from there, it would not be difficult to imagine that camera tilting and zooming through the window of an apartment and recording the activities of the individuals inside. If an individual fails to close the shades of his tenth floor apartment window, is anyone or anything in that apartment fair game for video surveillance?

The Supreme Court has recently eschewed an opportunity to establish the possibility of a legal challenge to video surveillance, at least on an individual level, in its decision in *United States v. Jones*.[197] The Court of Appeals for the District of Columbia had previously held that prolonged GPS surveillance violated a defendant's reasonable expectation of privacy.[198] During a joint investigation by the FBI and the District of Columbia's Metropolitan Police Department, the government planted a GPS tracking device on the appellant's car and monitored his travel over a month-long period.[199] The government used the evidence gleaned from the surveillance to convict him of trafficking in narcotics.[200] Jones argued before the D.C. Circuit that the extended period of surveillance had violated his Fourth Amendment reasonable expectation of privacy.[201] The D.C. Circuit agreed.[202] While the court did not disturb the general constitutionality of GPS surveillance, it did hold that such surveillance over the course of many weeks resulted in such an intimate picture of an individual's life as to violate a reasonable expectation of privacy.[203] The D.C. Circuit's reasoning suggests possible challenges to video surveillance in cases, for example, where a video camera is trained on a street (or on an entryway or window) to capture an individual's daily movements on an ongoing basis.

The Supreme Court unanimously affirmed the D.C. Circuit's ruling, but without offering support for the types of challenges to video surveillance suggested by the lower court's ruling.[204] The Court was divided on the reasoning for its decision, with the majority avoiding the reasonable expectation of privacy standard altogether. The majority opinion, authored by Justice Scalia, focused on the government's intrusion into private property

197. U.S. v. Jones, 132 S. Ct. 945 (U.S. 2011).

198. U.S. v. Maynard, 615 F.3d 544 (D.C. Cir. 2010).

199. U.S. v. Jones, 132 S. Ct. at 948.

200. *Id.*

201. *Maynard*, 615 F.3d at 555.

202. *Id.* at 563–64.

203. *Id.* at 560 ("[T]he whole of a person's movements over the course of a month is not actually exposed to the public because the likelihood a stranger would observe all those movements is not just remote, it is essentially nil. It is one thing for a passerby to observe or even to follow someone during a single journey as he goes to the market or returns home from work. It is another thing entirely for that stranger to pick up the scent again the next day and the day after that, week in and week out, dogging his prey until he has identified all the places, people, amusements, and chores that make up that person's hitherto private routine.").

204. U.S. v. Jones, 132 S. Ct. at 954 ("The judgment of the Court of Appeals for the D.C. Circuit is affirmed."); *id.* (Sotomayor, J., concurring) (joining the Court's opinion, but setting out different reasoning); *id.* at 957 (Alito, J., concurring) (joining the Court's opinion, but setting out different reasoning).

by placing the tracking device on Jones' car, rather than on the sustained nature of the surveillance.[205] The majority held that an individual's vehicle is an "effect," in which the individual has a right to be secure under the Fourth Amendment, and that the government violated the Fourth Amendment by "physically occup[ying] private property for the purpose of obtaining information."[206] Commentary immediately following the ruling has suggested that *Jones* indicates "a majority of the justices are prepared to apply broad Fourth Amendment privacy principles to bring the Fourth Amendment's ban on unreasonable searches into the digital age, when law enforcement officials can gather extensive information without ever entering an individual's home or vehicle."[207] It is true that in two concurring opinions by Justice Sotomayor and Justice Alito, five justices noted that much surveillance no longer relies upon physical intrusion of, for instance, a home, and that a modern interpretation of the reasonable expectation of privacy standard is needed.[208] However, the majority did not rely on this more modern view of the needs of Fourth Amendment protections, preferring a narrower ruling grounded in private property protections.[209]

The majority view differed significantly from the emphasis placed by Justice Sotomayor, in her concurring opinion, on the position that "the Fourth Amendment is not concerned only with trespassory intrusions on property."[210] Justice Sotomayor emphasized, "[A] Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable,"[211] and "does not turn upon the presence or absence of a physical intrusion."[212] Justice Sotomayor, along with Justice Alito in a separate concurrence, noted that technological advances, which enable nontrespassory surveillance techniques—that is, surveillance that does not depend on entry into, or attachment to, private property—will shape the evolution of society's privacy expectations.[213] The question that remains after *United States v. Jones* is how such expectations will evolve:

---

205. U.S. v. Jones, 132 S. Ct. 945 (U.S. 2011).

206. *Id.* at 949 ("The Fourth Amendment provides in relevant part that 'the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated.' It is beyond dispute that a vehicle is an 'effect' as that term is used in the Amendment.") (citing U.S. v. Chadwick, 433 U.S. 1, 12 (1977)) (some internal quotations omitted).

207. Adam Liptak, *Justices Say GPS Tracker Violated Privacy Rights*, N.Y. Times (Jan. 23, 2012), http://www.nytimes.com/2012/01/24/us/police-use-of-gps-is-ruled-unconstitutional.html?_r=2&hp.

208. *Jones*, 132 S. Ct. at 955 (Sotomayor, J, concurring); *id.* at 957 (Alito, J., concurring).

209. *Jones*, 132 S. Ct. at 949.

210. *Id.* at 954 (Sotomayor, J., concurring).

211. *Id.* (citing Kyllo v. U.S., 533 U.S. 27, 31–33 (2001)).

212. *Id.* at 955. (citing Katz v. U.S., 389 U.S. 347, 353 (1967)).

213. *Id.* ("[P]hysical intrusion is now unnecessary to many forms of surveillance."); *id.* at 957 (Alito, J., concurring) ("This case requires us to apply the Fourth Amendment's prohibition of unreasonable searches and seizures to a 21st-century surveillance technique.").

will new technology heighten the public's reasonable expectations of privacy, or will it do away with them altogether?

Indeed, the rapid development of new technology impacts all concerns related to video surveillance. In New York City, it is unclear how, when, and whether the City and law enforcement will adopt new surveillance programs and systems. For example, the NYPD's *Guidelines* currently state that the Domain Awareness System does not use facial recognition technology.[214] However, the *Guidelines* also state that technologies used by the System may "utilize or be integrated with systems and technologies deployed by other bureaus and divisions of the NYPD."[215] No guidelines exist to regulate what systems and technologies might be integrated through this clause, or how their utilizations or integrations might take place, leaving the field wide open for expansion and mission creep. In addition to the possible use of existing technologies that are not explicitly authorized, there is also the unanswered question of how new technologies will be adopted, and what limits may or may not be placed on their adoption.

### B. *Balancing Security, Privacy and Free Speech*

There are compelling and reasonable arguments in favor of video surveillance programs. But there are equally compelling and reasonable arguments for caution in implementing and maintaining them. The lack of public dialogue with regard to such systems should not be interpreted as a lack of concern; rather, it is more likely an indication of the limits of public knowledge about either the programs or the remarkable absence of public control over their operation. If surveillance cameras are to be ubiquitous, public education and dialogue are the only likely tools we have to monitor potential abuses and challenge them when they occur. The NYPD and city officials have had ample opportunity to take the lead in initiating public dialogue, but have failed to do so. One place for the public to start is in considering and advocating for legally enforceable regulations over video surveillance that would go further to protect privacy and First Amendment rights.

The City Council is the ideal starting point for regulating video surveillance in New York City, as it is well-positioned to facilitate public dialogue and to draft and pass legislation. The process of legislating regulations would require at least three key steps: (1) consideration and editing of the stated objectives of the LMSI/MMSI; (2) review of information regarding operations of the programs and determination of the most information that can safely be made public; and (3) determination of the most stringent privacy protections available without stripping the NYPD of its ability to keep the public safe. Such determinations require balancing a range of interests,

214. NYPD Guidelines, *supra* note 34, at 3.
215. *Id.*

which is why the City Council (which shares the interests of New Yorkers as well as the NYPD and its stakeholders) is better positioned than the NYPD (which has a clear perspective on one side of the debate) to set regulations. Regulations should clearly state the objectives of such programs; mandate public disclosure of much of the operations of the programs—particularly with regard to data storage, use, and sharing; and ensure the availability of legally cognizable claims regarding privacy violations and other abuses.

### 1. Clarifying Objectives

Much of the stated purpose of LMSI and MMSI is compelling, and hard to contradict. To observe "pre-operational activity by terrorist organizations," "aid in the detection of preparations to conduct terrorist attacks," "deter terrorist attacks," and "reduce incident response times" are all noble goals.[216] As Jeffrey Rosner explained, after he experienced an invasion of his privacy by the NYPD,[217] post-September 11th New Yorkers, like most Americans, generally favor the presence of cameras to deter another terrorist attack.[218] If the *Guidelines*' Statement of Purpose set out solely the goals above, there would likely be little to debate, at least with regard to objectives.

However, two key facets of the Statement of Purpose are vague and confusing, and it is difficult to connect them with the other four points. First, it is not clear what is meant by "provid[ing] a degree of common domain awareness for all Stakeholders,"[219] nor why doing so is important. Second, it is not clear what is meant by "creat[ing] a common technological infrastructure to support the integration of new security technology,"[220] nor what the parameters of such an infrastructure and new technology might be.

The first point, providing common domain awareness for all stakeholders in the LMSI/MMSI, is concerning for two reasons. The NYPD has integrated private entities into City security and surveillance programs[221] with little to no public disclosure or dialogue. The NYPD has not shared its reasons for doing so, nor has it shared any standards it uses to determine which private entities to integrate. It is not clear what, if any, vetting process

216. NYPD Guidelines, *supra* note 34, at 2–3.

217. *See* Dwyer *supra* note 145.

218. *See, e.g.*, John Esterbrook, *Poll: Americans OK with Video Scrutiny*, CBS NEWS (Feb. 11, 2009), http://www.cbsnews.com/stories/2002/04/21/opinion/polls/main506822.shtml (stating that Americans are willing to "put up with" surveillance cameras in public places, and "feel, by a three-to-one margin (72%–24%), that they will have to give up some of their personal freedoms in order to make the country safe from terrorist attacks"); Michelle Lirtzman, *Poll: Surveillance Cameras*, ABC NEWS (Jul. 29, 2007), *available at* http://abcnews.go.com/images/US/1041a5Surveillance.pdf (reporting that Americans support the increased use of surveillance cameras by almost a three-to-one margin).

219. NYPD Guidelines, *supra* note 34, at 3.

220. *Id.*

221. NYPD Press Release (noting the establishment of workstations in the Lower Manhattan Security Coordination Center for "the NYPD's various public and private partners").

may be utilized to screen stakeholders or to hold them accountable to the limited regulations the NYPD enforces over the program. Further, the NYPD also has not set out how "a degree of common domain awareness" is identified, and why it is important for private entities to share the level of security awareness that the NYPD enjoys.[222]

Integrating private entities into public safety programs opens such programs to conflicting purposes and priorities. It also may increase opportunities for misuse of data and privacy violations due to expanding access to such data to a variety of parties with differing interests, objectives, and levels of experience. Such integrations should not be undertaken without public awareness and legislative approval.

The second point, creating a common technological infrastructure to support the integration of new security technology, is troubling for related reasons. First, it is unclear with whom the infrastructure is to be "common." The *Guidelines* do not state whether it is to be common as between the NYPD and its private stakeholders, or whether there are other entities—such as federal investigative agencies—that are also included. Second, there are no boundaries established with regard to the integration of new security technology, leaving the field wide open for the NYPD, its private stakeholders, and any other unnamed partners, to experiment with new technologies without informing the public. For instance, as discussed above, while the *Guidelines* assure that facial recognition technology will not be used as part of the Domain Awareness System,[223] it is not at all clear that the NYPD and its stakeholders can be prevented from using such technology, should it be deemed an important new security technology to integrate. As surveillance technology develops quickly in the twenty-first century, it appears that the *Guidelines* have created an open platform for experimentation without any mandate to provide public notice.

Objectives for the LMSI/MMSI (as well as for any public surveillance program) can only be set responsibly through dialogue with the public. In the case of the *Guidelines*, there were no public hearings held to provide New Yorkers with a chance to understand the new programs, ask questions, raise concerns, and present goals and boundaries.[224] The *Guidelines* were made public on the New York City Police Department's website for one month prior to their adoption, and a press release provided an NYPD email address to which concerns and questions could be directed.[225] Less than 100 comments were made, which has caused at least one City official to claim that New Yorkers were not concerned about either the *Guidelines* or the

222. NYPD Guidelines, *supra* note 34, at 3 (providing for "common domain awareness" but refraining from defining the term or clarifying its meaning).

223. *Id.*

224. *See* Dunn Letter, *supra* note 188.

225. Press Release, N.Y.C. Police Dep't, New York City Police Department Releases Draft of Public Security Privacy Guidelines for Public Comment (Feb. 25, 2009), *available at* http://www.nyc.gov/html/nypd/html/pr/pr_2009_005.shtml.

LMSI/MMSI program.[226] It is not necessarily the case, however, that so few comments are evidence of a lack of concern. It is also possible that most New Yorkers do not learn of events in their city from NYPD press releases, and that many members of the public were unaware of the *Guidelines* during the period provided for review and comment. It is also possible that those New Yorkers who were aware of the public comment period were discouraged from sharing comments directly with the New York City Police Department, for fear of being identified and targeted. It is for this reason that such processes are best placed into the hands of legislators; in such cases, the processes may at the very least become a matter of public record, providing for some amount of accountability, and at best they may be opened to meaningful public debate and dialogue.

### 2. Providing Information

Information about the operations of the LMSI/MMSI has been very limited and difficult to come by. Following the New York State Supreme Court's 2009 and 2010 rulings, the NYPD is exempted from having to produce any documents involving "the operational details of the LMSI, such as the types of information to be collected and how the information will be used, shared and stored and for how long,"[227] as well as any communications within and between agencies and stakeholders involved in the LMSI.[228] It is certainly reasonable that some operational details of security programs must be kept confidential in the interest of public safety. However, information regarding the length of time data may be stored and rules regulating its use are of great concern to members of the public, who are directly impacted by such regulations. Similarly, information about the process by which security systems such as the LMSI/MMSI were initiated, almost certainly captured in communications between the NYPD and stakeholders, is of great interest to the public. Such information promises to shed greater light on the most salient internal objectives of the programs, in comparison to the vague objectives presently shared with the public. It also provides room for the public to question such objectives, and the strategies set for achieving them.

For example, the *Guidelines* provide that all personnel in the Lower Manhattan Security Coordination Center are required to undergo privacy training.[229] However, the public has not received any clear information regarding what type of training is required. It appears that the training course is a three-hour-long program developed by a private contractor who tailored the course specifically to the NYPD's system with "practical real-world examples," clearly setting out "privacy principles."[230] It may be true that this

226. Anonymous Interview, *supra* note 9.
227. New York Civil Liberties Union, 242 N.Y.L.J. at 9–10 (2009).
228. New York Civil Liberties Union, No. 112145.
229. NYPD Guidelines, *supra* note 34, at 6–7.
230. Anonymous Interview, *supra* note 9.

program is highly effective in training NYPD and stakeholder personnel to value and protect the privacy of New Yorkers. The program may effectively help them to identify and balance precarious situations in which security interests and privacy interests must be carefully weighed. But there is no information publicly available about the program to truly reassure those who are subject to video surveillance in the City, such as what "privacy principles" are communicated, what examples trainees are given to help them identify situations in which they must prioritize privacy, and how personnel are monitored and assessed.[231] In the case of Paris Lane, for instance, Commissioner Kelly asserted in the aftermath of the scandal that the NYPD had regulations in place to protect tenants' privacy and that VIPER Unit officers were trained and supervised.[232] Whatever training that occurred did little to protect the privacy of Paris Lane and his family. Similarly, the current lack of information about privacy training in the Lower Manhattan Security Coordination Center does little to engender trust among surveilled New Yorkers. It also does little to provide accountability when privacy principles are breached.

A further example of the type of highly relevant information withheld from the public is the management of the retention and use of data collected from surveillance cameras. The *Guidelines* state that video data is destroyed after thirty days, and it has been suggested by at least one City official that a thirty-day deletion policy is unprecedented and an important concession for privacy protection.[233] However, recent surveillance history in New York City suggests otherwise. Again, in the case of Paris Lane, the policy of the VIPER program was to store videotapes in secure locations and to destroy or erase them after fourteen days.[234] The fourteen-day deletion policy was more stringent than the LMSI/MMSI's thirty-day deletion policy; however, it still allowed for privacy violations. This example suggests that time-based retention policies are not sufficient to secure the data of New Yorkers. There must be clear regulations that detail how such data is stored, who has access to it, how it may be accessed, and under what circumstances it may be utilized. The *Guidelines* make vague statements that gesture toward regulating these elements, but provide no concrete information. Even assuming that clear and stringent regulations are in place and cannot be revealed due to security concerns, it should be possible that more information might be

231. NYPD Guidelines, *supra* note 34, at 7 (stating that all personnel in the Lower Manhattan Security Coordination Center will undergo "periodic assessments" related to their privacy training).

232. New York Civil Liberties Union, 242 N.Y.L.J. at 3 (citing letter from Raymond W. Kelly to C. Virginia Fields, Apr. 27, 2004, on file with the NYCLU).

233. Anonymous Interview, *supra* note 9 (stating that a thirty-day deletion policy has "significant implications" for potentially hindering police work, but that it was a concession made to privacy concerns).

234. New York Civil Liberties Union, 242 N.Y.L.J. at 3 (citing letter from Raymond W. Kelly to C. Virginia Fields, Apr. 27, 2004, on file with the NYCLU).

provided beyond the statement that use is permitted "in furtherance of the purposes set out in the Statement of Purpose."[235] New Yorkers should be assured that there is a chain of command, that supervisors are on hand to authorize any use or retention of data, and that substantial protections are in place to prevent unauthorized use or retention of data.

These examples demonstrate that voluntary self-regulatory guidelines adopted by the NYPD are insufficient in establishing the privacy rights of New Yorkers. The *Guidelines* do not provide assurance that meaningful measures are in place to protect New Yorkers' privacy. For this reason, it is preferable for the City Council to adopt regulations that are binding on the NYPD and its stakeholders. Legislation provides the most promising means of establishing clear objectives for surveillance programs that balance security concerns against other public interests, establishing regulations for the retention, use, and sharing of data and monitoring the interaction between the NYPD and private stakeholders. Legislation is also the best means of ensuring that the regulations are made public and that the public is given meaningful opportunity to discuss and debate the measures before they are implemented. While legislation did not precede the implementation of the LMSI/MMSI, it is not too late to effect legislation to regulate these security systems.

### 3. Ensuring Protections

In 2006, the NYCLU set out a list of recommendations for making video surveillance more accountable to the public.[236] These recommendations have not been addressed by the NYPD, the City Council, or even the media, but they are useful in offering key provisions that might be included in City legislation regulating video surveillance. The key provisions are: (1) the establishment of "specific and justifiable" objectives for surveillance programs; (2) public notice in areas where video cameras are currently, or are planned to be, installed; (3) a guarantee that personnel operating or controlling access to surveillance cameras and data are properly trained and supervised; (4) the establishment of clear rules and procedures for the retention, storage, and destruction of video surveillance images; and (5) the explicit prohibition of unlawful practices with regard to video surveillance cameras, with legal penalties for violations.[237]

In establishing objectives for video surveillance programs, the City should undertake needs assessments prior to the installation of cameras, and make those assessments public and open to public discussion. Any legislation should also provide for regular audits to determine the ongoing efficacy of video surveillance and the programs' compliance with laws and regula-

235. NYPD Guidelines, *supra* note 34, at 4–5.
236. WHO'S WATCHING?, *supra* note 15, at 13.
237. *Id.* at 13–16.

tions. The City and the NYPD may have already undertaken such assessments, but they have not been required to produce documentation, so it is impossible for the public to gain substantive knowledge about the objectives of New York City's video surveillance programs, and the status of those objectives. Further, legislation should require public notice in neighborhoods and areas where video cameras will be—or are currently—installed. The *Guidelines* do set out a notification requirement;[238] however, since the *Guidelines* are not legally enforceable, there is no guarantee that cameras are consistently marked. The process of public notice should also provide residents meaningful opportunities to participate in decisions regarding location and operation of cameras. Signs indicating the presence of cameras are insufficient. The NYPD and the City government should undertake public education, and hold public hearings in areas where cameras are or will be placed, to inform residents about the scope of the cameras, and allow them the opportunity to air concerns, and learn what legal processes and protections may or may not be available to them.

City legislation must require that individuals charged with operating or controlling access to video surveillance cameras will be properly trained and closely supervised, and should set out regulations addressing the number of hours of training required, the subjects to be covered in training sessions, the regularity of trainings and assessments, and the standards to be met in assessing both training programs and the actions of personnel. Given prior incidents that would reasonably dissolve public confidence in their police to properly execute such programs, the public should be assured that a high-level of training and supervision is in place and that changes have been made since the most recent reported incidents. Legislation must also clarify a chain of command and set out processes for approval by establishing clear rules and procedures for the retention, storage, and destruction of video surveillance images. The *Guidelines* set out some standards with regard to these issues, but they permit each standard to be overridden on a case-by-case basis, without a standard for public disclosure of the process for an override.[239] This is insufficient and should be addressed by legislation. Finally, the City must provide legal penalties for violations of its regulations. It is not sufficient for the NYPD to set out a series of unenforceable *Guidelines*; regulations must be legally enforceable in order to be meaningful, and legislation should be passed to ensure that they are.

## Conclusion

There are legitimate security concerns—both local and national—that offer compelling reasons for the use of video surveillance programs. The purpose of this Note has not been to challenge them; rather, it has been to

238. NYPD Guidelines, *supra* note 34, at 3.
239. *Id.*

highlight the problems that emerge when information about such programs is withheld from the public in the name of national security, when oversight policies are vague and unenforceable, and when no legal mechanism exists to hold public institutions accountable for violations. Only through clear objectives, public education, and the ability to legally enforce standards for the use of surveillance technologies will the public be able to challenge surveillance that encroaches on privacy, First Amendment rights, and basic dignity. A case in point is the controversy over the Transportation Security Administration (TSA)'s newly invasive security screening policies that were deployed towards the end of 2010.[240] Only after vehemently negative public reaction did the TSA begin to back off its previous hardline position. In the wake of public calls for protests that would have crippled the United States' air transportation system during Thanksgiving weekend, the TSA suggested that the program "will be adapted as conditions warrant," to make them "as minimally invasive as possible, while still providing the security that the American people want and deserve."[241]

There has been no such public reaction to video surveillance cameras in New York City, very likely because the program is not as publicly recognizable as a security screening program implemented in airports across the nation. To date, the only available challenge to surveillance cameras must come as a response to specific, individual cases of privacy violation, discrimination, or the chilling of free speech. Such challenges depend on individuals to recognize a violation and to have the courage and resources to come forward and bring a challenge, without any guarantee of legal recourse. In such cases, post-violation complaints and litigation cannot be fully satisfying to those whose privacy, speech protections, or dignity have been violated. Even victories in court cannot make such individuals fully whole. Without enforceable regulations and legislation, at least at the local level, New Yorkers will be subject to unchecked surveillance that will only expand as technology produces more and more options.

240. Susan Stellin, *Pat-Downs at Airports Prompt Complaints*, N.Y. TIMES (Nov. 19, 2010), http://www.nytimes.com/2010/11/19/business/19security.html?ref=transportation_security_administration.

241. Mike Allen, *TSA Chief: Screening May Evolve*, POLITICO (Nov. 21, 2010), http://www.politico.com/news/stories/1110/45460.html.