PRIVACY PROTESTS: SURVEILLANCE EVASION AND FOURTH AMENDMENT SUSPICION

Elizabeth E. Joh*

The police tend to think that those who evade surveillance are criminals. Yet the evasion may only be a protest against the surveillance itself. Faced with the growing surveillance capacities of the government, some people object. They buy "burners" (prepaid phones) or "freedom phones" from Asia that have had all tracking devices removed, or they hide their smartphones in ad hoc Faraday cages that block their signals. They use Tor to surf the internet. They identify tracking devices with GPS detectors. They avoid credit cards and choose cash, prepaid debit cards, or bitcoins. They burn their garbage. At the extreme end, some "live off the grid" and cut off all contact with the modern world.

These are all examples of what I call privacy protests: actions individuals take to block or to thwart government surveillance for reasons unrelated to criminal wrongdoing. Those engaged in privacy protests do so primarily because they object to the presence of perceived or potential government surveillance in their lives. How do we tell the difference between privacy protests and criminal evasions, and why does it matter? Surprisingly scant attention has been given to these questions, in part because Fourth Amendment law makes little distinction between ordinary criminal evasions and privacy protests. This Article discusses the importance of these ordinary acts of resistance, their place in constitutional criminal procedure, and their potential social value in the struggle over the meaning of privacy.

---

* Professor of Law, University of California, Davis, School of Law (eejoh@ucdavis.edu). Thanks to Ash Bhagwat, Timothy Casey, Jack Chin, Ed Imwinkelried, Wayne Logan, Charles Reichmann, Chris Soghoian, and participants in the 2013 Privacy Law Scholars Conference for their helpful comments and suggestions, to the librarians at the Mabie Law Library and Lindsey Peterson for their research assistance, and to the U.C. Davis School of Law for institutional support.

TABLE OF CONTENTS

INTRODUCTION

The police tend to think those who evade surveillance are criminals. Yet the evasion may only be a protest against the surveillance itself. How do we tell the difference, and why does it matter? Surprisingly, legal commentators and judges have not given these questions serious attention.[1]

We should be especially surprised because the surveillance capacities of the police have expanded dramatically. These technologies have made it possible for government surveillance to become more pervasive, bureaucratic, and routinized.[2] The federal government anticipates that the near future will bring

---

1. Sociologists, however, most notably David Lyon and Gary Marx, have written about the potential significance of surveillance resistance. *See, e.g.*, DAVID LYON, SURVEILLANCE STUDIES: AN OVERVIEW 178 (2007) (observing that only consideration of "the myriad forms of spontaneous [and] ad hoc . . . opposition to and negotiation of surveillance" will provide "a much more nuanced and subtle picture" of surveillance dynamics) (emphasis omitted). Even within surveillance studies, some have criticized the insufficient attention paid to the "resistance to surveillance." *See, e.g.*, Aaron K. Martin et al., *Understanding Resistance to Digital Surveillance: Towards a Multi-Disciplinary, Multi-Actor Framework*, 6 SURVEILLANCE & SOC'Y 213, 214 (2009).

2. Nick Bilton, *Disruptions: Shields for Privacy in a Smartphone World*, N.Y. TIMES, June 25, 2012, at B5 (citing Professor David D. Cole, professor of constitutional and national security law at Georgetown University, as stating that the government sees "tremendous possibilities in technology" to deter and to detect crime).

wider adoption of facial recognition software and domestic surveillance drones.[3] Iris-scanners are already being used by the Department of Homeland Security, the American military, the NYPD, and police departments around the country.[4] Dozens of American cities have adopted Shotspotter technology: sophisticated listening devices designed to identify the location of gunshot sounds within forty feet.[5] Cities like San Francisco, Baltimore, and Columbus have installed audio surveillance systems on public buses that are capable of recording and storing conversations.[6] Other cities, like New York, Miami, and Los Angeles, are adopting or considering the adoption of an extensive network of surveillance cameras

---

3. The FTC recently published "best practices" guidelines for facial recognition software, a gesture seen as a sign that such software will become much more widespread. *See* FED. TRADE COMM'N, FACING FACTS: BEST PRACTICES FOR COMMON USES OF FACIAL RECOGNITION TECHNOLOGIES (2012). In addition, the FBI is currently developing an expansion of its identification systems—currently based on fingerprints—to include facial recognition and other biometric data as part of its Next Generation Identification Program. *See* Sara Reardon, *If the Feds Fit the Face*, NEW SCIENTIST, Sept. 1, 2012, at 20. On the federal approval for more widespread use of unmanned drones in the U.S., see FAA Modernization and Reform Act of 2012, Pub. L. No. 112-95 § 332 (2012) (requiring FAA to promulgate rules on licensing drones for public safety agencies and to develop a plan to "safely accelerate" the integration of drone operation into the National Airspace System no later than 2015); *see also* Brian Bennett, *Police Departments Wait for FAA Clearance to Fly Drones*, L.A. TIMES (Apr. 29, 2012), http://articles.latimes.com/2012/apr/29/nation/la-na-drone-faa-20120430 (noting that "[t]housands of remotely piloted aircraft of various shapes, sizes and speeds . . . may soon be buzzing overhead"); Andy Pasztor, *U.S. Skies Could See More Drones*, WALL ST. J., Feb. 4, 2012, at A7 (predicting that drones could be used for "environmental monitoring, fire protection and surveillance of suspected criminals").

4. Iris scanners identify individuals based on the unique patterns found in every person's iris. The NYPD began scanning the irises of every person arrested in Manhattan in 2010. The technology is considered less intrusive than retinal scanning, which may reveal health conditions of the person scanned. *See* Thomas Frank, *U.S. to Test Iris Scan Technology*, USA TODAY, Sept. 13, 2010, at 01A (citing test adoption of iris scanners at border patrol sites); Nicole Perlroth, *Finding the Unique in You to Build a Better Password*, N.Y. TIMES (Dec. 23, 2011), http://bits.blogs.nytimes.com/2011/12/23/finding-the-unique-in-you-to-build-a-better-password/?_r=0 (stating that "dozens" of police departments that have already adopted iris scanning technology); Ray Rivera & Al Baker, *To Prevent Escapes, Police Start Scanning Irises of Suspects*, N.Y. TIMES, Nov. 16, 2010, at A24 (citing use by NYPD and military); *see also* Michael Winter, *Big Brother: Eye-Scanners Being Installed Across One Mexican City*, USA TODAY (Aug. 19, 2010), http://content.usatoday.com/communities/ondeadline/post/2010/08/big-brother-eye-scanners-being-installed-across-one-mexican-city-/1#.UlHv8YbYeSo (describing announcement that city of Leon, Mexico will install iris scanners to create "the most secure city in the world").

5. *See* Cara Buckley, *High-Tech 'Ears' Listen for Shots*, N.Y. TIMES, Nov. 22, 2009, at MB1 (describing technology as providing operators with "near-bionic listening powers"). Shotspotter can also pick up conversations, as in the case of a recorded argument that led to an alleged murder, and might be used as evidence. *See* Erica Goode, *Gunfire Is Heard and Pinpointed, but Technology Is Argued over*, N.Y. TIMES, May 29, 2012, at A13 (describing facts from criminal case in New Bedford, Massachusetts).

6. *See* Michael Brick, *Big Brother's Listening*, THE DAILY (Dec. 10, 2012) (on file with author),.

directed at public spaces, just as the city of London has already established.[7] Ordinary American life today cannot be easily lived without being targeted by government surveillance.[8] Many, if not most, people acquiesce to these demands for information about them, either out of acceptance or resignation.[9]

But some people object. They take steps to *thwart* police surveillance, not because they are seeking to conceal criminal acts, but out of ideological belief or personal conviction.[10] Advice on "surveillance defense" and counter-surveillance products is readily available on the internet:[11] Use Tor to surf the internet.[12] Encrypt your digital communications.[13] Use disposable "guerilla email" addresses and disposable phone numbers.[14] Avoid ordinary credit cards and choose only cash, prepaid debit cards, or bitcoins to make a financial trail harder to detect. Avoid cell phones unless they are "burners" (prepaid phones), "dumb phones," or

---

7. While some dispute exists as to the exact number, there are at least 8,000 cameras used by police in London and its surrounding boroughs, and at least 500,000 total from private and public sources. Rebecca J. Rosen, *London Riots, Big Brother Watches: CCTV Cameras Blanket the U.K.*, THE ATLANTIC (Aug. 9, 2011, 3:30 PM), http://www.theatlantic.com/technology/archive/2011/08/london-riots-big-brother-watches-cctv-cameras-blanket-the-uk/243356/. It is commonly said that the U.K. has the greatest number of CCTV cameras in use on a per capita basis. *See, e.g.*, Steve Stecklow et al., *Watch on the Thames*, WALL ST. J., July 8, 2005, at B1 (noting that the British police also monitor private camera systems). In 2012, the NYPD confirmed that it was using a network of 3,000 cameras and 100 license plate readers as a part of its Domain Awareness System, which permits the police to gather data instantly on suspicious activity such as parcels and vehicles. Chau Lam, *NYPD Unveils Computerized Surveillance System*, NEWSDAY, Aug. 9, 2012.

8. Of course, the modern state must collect some information from its citizens to govern at all, but rapid advances in technology have amplified the number and sources of data collected. *See* David Garland, *Panopticon Days*, 20 CRIM. JUSTICE MATTERS 3, 3–4 (1995).

9. *See, e.g.*, David Lyon, *Resisting Surveillance*, *in* THE SURVEILLANCE STUDIES READER 368, 373 (Sean P. Hier & Josh Greenberg, eds., 2007) ("Compliance with surveillance is commonplace.").

10. At the other end of the behavioral spectrum, some people *curb* their behavior precisely to avoid police suspicion, even if they have done nothing wrong. For provocative analysis of the issue, see generally L. Rush Atkinson, *The Bilateral Fourth Amendment and the Duties of Law-Abiding Persons*, 99 GEO. L. J. 1517 (2011).

11. *See* Bilton, *supra* note 2 (observing that "companies . . . have an incentive to create technologies that protect citizens from their government and deter officials from documenting our every movement").

12. *See Tor: Overview*, TOR, www.torproject.org/about/overview.html.en (last visited Oct. 6, 2013); *see also* Catherine Price, *The Anonymity Experiment*, POPULAR SCI., Mar. 1, 2008, at 60 (noting that some online companies provide similar fee-based services for online anonymity).

13. *See, e.g.*, Jenna Wortham, *Seeking Online Refuse from Spying Eyes*, N.Y. TIMES (Oct. 19, 2013, 4:24 PM), http://bits.blogs.nytimes.com/2013/10/19/seeking-online-refuge-from-spying-eyes/?smid=pl-share.

14. *See* Stephanie Mlot, *Create Disposable Phone Numbers with Burner iPhone App,* PC MAG ONLINE (Aug. 9, 2012, 10:32 AM), http://www.pcmag.com/article2/0,2817,2408265,00.asp.

"freedom phones" from Asia that have had all tracking devices removed. Alternatively, hide your smartphone in an ad hoc Faraday cage, like a refrigerator, to avoid being tracked.[15] Use photoblocker film on a license plate or a ski mask to thwart a red-light camera.[16] Use a Spyfinder camera detector to see if someone is watching you.[17] Use "spoof cards" that mask your identity on caller identification devices.[18] Burn your garbage[19] to hamper investigations of your financial records or the collection of your genetic information.[20] Hire a professional to alter your digital self on the internet by erasing data or posting multiple false identities.[21] At the extreme end, you could live "off the grid" and cut off all contact with the modern world.[22]

---

15. A Faraday cage shields its interior from external electric fields such as radio signals. *See, e.g.* Kelsey D. Atherton, *Hide from GPS with This Signal-Blocking Phone Case,* POPULAR SCI. (Aug. 6, 2013, 1:15 PM), http://www.popsci.com/gadgets/article/2013-08/how-protect-yourself-your-phone. NSA document leaker Edward Snowden reportedly asked visitors to place their cellphones in his refrigerators so as to block their signals. *See* Heather Murphy, *The Lede: Why Snowden Asked Visitors in Hong Kong to Refrigerate Their Phones*, N.Y. TIMES BLOG (June 25, 2013, 9:41 AM), http://thelede.blogs.nytimes.com/2013/06/25/why-snowdens-visitors-put-their-phones-in-the-fridge/.

16. *See* Don Oldenburg, *Drivers Try an Anti-Photo Finish*, WASH. POST, July 21, 2004, at A01; Brad Tuttle, *Big Brother Backlash: Citizens Unite to Bring Down Ticket-Generating Red-Light Cameras*, TIME (Feb. 16, 2012), http://business.time.com/2012/02/16/big-brother-backlash-citizens-unite-to-bring-down-ticket-generating-red-light-cameras/ (reporting of a man who wore a monkey mask while driving).

17. Spyfinder is just one of the camera detection devices available on the internet. *See* TOTAL SEC., INC., http://www.spysource.net/spyfinder.htm (last visited Oct. 6, 2013).

18. *See* FRANK M. AHEARN & EILEEN C. HORAN, HOW TO DISAPPEAR 93 (2010).

19. Professional skip tracer Frank Ahearn advises those wishing to "disappear" to follow one simple rule: "When you're done with it, destroy." *Id.* at 134.

20. There have been a number of instances in which either the police or private investigators have found valuable genetic evidence on discarded objects such as dental floss and eating utensils. For example, the man accused of being the "grim sleeper" serial killer in Los Angeles was arrested after the police obtained a DNA sample from discarded food items. Franklin became a suspect after crime scene DNA was linked to DNA that his son Christopher provided. Jennifer Steinhauer, *'Grim Sleeper' Arrest Fans Debate on DNA Use*, N.Y. TIMES, July 9, 2010, at A14. For other examples, see generally Elizabeth E. Joh, *Reclaiming "Abandoned" DNA: The Fourth Amendment and Genetic Privacy*, 100 NW. U. L. REV. 857 (2006).

21. *See* AHEARN & HORAN, *supra* note 18, at 11–26 (discussing the task of the "skip tracer" who finds clues to trace an individual's whereabouts).

22. See Price, *supra* note 12, at 60 (advising those seeking privacy to pay in cash; avoid use of cellphones, landlines, and email; avoid government buildings and airports; wear a hat and sunglasses; avoid automatic toll lanes; refuse to buy plane tickets, rent cars, etc.); *cf.* Sarah Jacobsson Purewal, *Erase Yourself from the Web*, PC WORLD (Mar. 30, 2011, 6:00 PM), http://www.pcworld.com/article/223682/erase_your_web_presence.html (noting that "the best way to 'erase' yourself from the Internet is never to have been on it in the first place").

These are all examples of what I call *privacy protests*: actions individuals may take[23] to block or thwart surveillance from the police for reasons that are unrelated to criminal wrongdoing.[24] Unlike people who hide their activities because they have committed a crime, those engaged in privacy protests do so primarily because they object to the presence of perceived or potential government surveillance.[25] People engage in these protests for all kinds of reasons, whether these reasons are political, philosophical, idiosyncratic, or just paranoid. These protests are not necessarily the work of extremists, either. The revelation in June 2013 that the National Security Agency has been collecting the telephone records of millions of Americans[26] prompted both calls for greater oversight as well as numerous mainstream media articles providing advice on avoiding government surveillance.[27]

---

23. These are noncriminal actions; I exclude instances where individuals are motivated by concerns about government surveillance but engage in criminal activity to protest it, such as destroying surveillance cameras, buying surveillance detection equipment whose possession is illegal, and so on. This definition also excludes actions artists take to protest government surveillance in ways that are obviously works of art (also known as *surveillance art*). Because they do not resemble criminal actions, these acts do not raise the same sorts of problems as true privacy protests. For instance, the Surveillance Camera Players perform plays in front of surveillance cameras to draw attention to them. *See* SURVEILLANCE CAMERA PLAYERS, http://www.notbored.org/the-scp.html (last visited Oct. 6, 2013). Notably, some artists also engage in criminal acts as part of their art, including "video sniffing," which involves tapping into a CCTV network and hacking into surveillance networks and broadcasting the images for unintended audiences. *See, e.g.*, Christopher Werth, *Watching the Watchers*, NEWSWEEK, Oct. 20, 2008, at E4 (describing European artists participating in both types of art). In the U.K., the artist known as "Banksy" has become identified with an antisurveillance art campaign, particularly his graffiti art "One Nation Under CCTV." *See* Liz Logan, *Banksy Defends His Guerrilla Grafitti Art*, TIME ENT. (Oct. 29, 2008), http://content.time.com/time/arts/article/0,8599,1854616,00.html.

24. Sociologist Gary Marx identified eleven types of "surveillance neutralization" individuals use to avoid surveillance from all sources, not just the police. *See* Gary Marx, *A Tack in the Shoe: Neutralizing and Resisting the New Surveillance*, 59 J. SOCIAL ISSUES 369, 374 (2003). Marx's perceptive insights into the same phenomenon I discuss here, however, do not include a discussion of their implications for the law or legal scholarship. *See id.*

25. The *hacker community* is probably most vocal in its efforts to defend against electronic surveillance, but these are not meaningfully different than low-tech efforts.

26. *See* Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, THE GUARDIAN (June 5, 2013), http://www.guardian.co.uk/world/2013/jun/06/nsa-phone-records-verizon-court-order.

27. *See, e.g.*, Timothy B. Lee, *Five Ways to Stop the NSA from Spying on You*, WONKBLOG (June 13, 2013), http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/10/five-ways-to-stop-the-nsa-from-spying-on-you/; Victor Luckerson, *The Anonymous Internet: Privacy Tools Grow in Popularity Following NSA Revelations*, TIME (June 20, 2013), http://business.time.com/2013/06/20/the-anonymous-internet-privacy-tools-grow-in-popularity-following-nsa-revelations/ (reporting that online privacy tools have reported unusual demand after NSA controversy); Raphael Satter, *How to Avoid Snooping by the NSA Prism Program*, SAN JOSE MERCURY NEWS, (June 14, 2013, 9:29 PM)

Those unhappy with a governmental policy have many options, most of them more socially accepted than the acts described here. For many, social change takes the form of lobbying a legislator, organizing a grassroots campaign, or harnessing social media for one's cause. Yet in one sense, privacy protests function in the same way as these activities because they involve expressions of protest against what individuals feel is governmental overreach. However, privacy protests differ from more conventional forms of protest because of their individualistic and ad hoc nature. As government surveillance capabilities expand, privacy protests may become an even more important form of social action.

Yet, for the police, privacy protests are easily grouped together with the evasive actions that those who have committed crimes take.[28] The evasion of police surveillance may look the same whether perpetrated by a criminal or a privacy protestor.[29] Tor, an encryption tool that permits near-anonymous use of the internet, is used both by those who value digital privacy and by criminals.[30] For this reason, privacy protests against the police and the government have been largely underappreciated within the criminal law literature.

Because they are not limited to antitechnology protests, many seemingly dissimilar acts ought to be considered privacy protests. At first glance, a teenager in Brownsville, New York[31] who always avoids the police no matter what he is doing shares little in common with a libertarian-minded internet user who scrupulously erases his digital trails. Yet each of these actions may be similar in

---

http://www.mercurynews.com/business/ci_23461010/how-avoid-snooping-by-nsa-prism-program; Mathew J. Schwartz, *7 Tips to Avoid NSA Digital Dragnet*, INFO. WEEK, (June 12, 2013, 1:23 PM), http://www.informationweek.com/security/privacy/7-tips-to-avoid-nsa-digital-dragnet/240156535; Somini Sengupta, *Digital Tools to Curb Snooping*, N.Y.TIMES, July 18, 2013, at B1 (observing that "short of living in a cave without a cellphone," protecting personal information online is difficult); Natasha Singer, *Ways to Make Your Online Tracks Harder to Follow*, N.Y. TIMES, June 19, 2013, at F4; Daniel Stuckey, *The Motherboard Guide to Avoiding the NSA*, MOTHERBOARD, http://motherboard.vice.com/blog/the-motherboard-guide-to-avoiding-the-nsa/ (last visited Oct. 6, 2013).

28. Gary Marx makes a similar point. *See supra* note 24, at 374 (noting that there are "likely common resistance moves shared by a citizen concerned with protecting personal privacy and a criminal seeking to avoid detection").

29. *See infra* Part I.

30. Charlotte Philby, *The Tor System: Welcome to the Dark Internet Where You Can Search in Secret*, INDEP. (June 10, 2013), http://www.independent.co.uk/news/media/online/the-tor-system-welcome-to-the-dark-internet-where-you-can-search-in-secret-8651364.html.

31. Brownsville has been a central target of the NYPD in its controversial stop and frisk policies. *See, e.g.,* Ray Rivera et al., *A Few Blocks, 4 Years, 52,000 Police Stops*, N.Y. TIMES, July 12, 2010, at A1. A federal district court judge recently decided that the same policies violated the Fourth Amendment rights of those stopped. *See* Joseph Goldstein, *Judge Rejects New York's Stop-and-Frisk Policy*, N.Y. TIMES, Aug. 13, 2013, at A1.

intention and function.[32] How we consider one act should inform how we consider the other.

Moreover, these protests share a pedigree with more recognizable concerns about governmental overreaching. While the Supreme Court has not recognized privacy protests in particular, many justices over time have noted that our constitutional traditions reflect suspicions about overzealous government surveillance.[33] Even in 1966, Supreme Court Justice William Douglas famously raised the concern that we were already "rapidly entering the age of no privacy, where everyone is open to surveillance at all times; where there are no secrets from government."[34]

Though these "everyday forms of resistance make no headlines,"[35] we should not ignore privacy protests, for they reveal social understandings of privacy and can inform how we justify government surveillance. There are, of course, many organizations (civil liberties groups, professional associations, and other government agencies) that monitor and speak out against privacy intrusions that the government commits, but this Article focuses on individuals and their attempts

---

32. That the consideration of race may play a factor in these kinds of stops is an important concern, and it has been the primary basis in the scholarly literature for discussing evasive behavior in this context. *See, e.g.*, Amy D. Ronner, *Fleeing While Black: The Fourth Amendment*, 32 COLUM. HUM. RTS. L. REV. 383 (2001).

33. *See, e.g.*, California v. Ciraolo, 476 U.S. 207, 217 (1986) (Powell, J., dissenting) (noting that the Fourth Amendment "reflects a choice that our society should be one in which citizens 'dwell in reasonable security and freedom from surveillance'" (quoting Johnson v. United States, 333 U.S. 10, 14 (1948))); Goldman v. United States, 316 U.S. 129, 139 (1942) (Murphy, J., dissenting) (observing that "science has brought forth far more effective devices for the invasion of a person's privacy than the direct and obvious methods of oppression which were detested by our forebears and which inspired the Fourth Amendment"), *overruled in part by* Katz v. United States, 389 U.S. 347 (1967).

34. Osborn v. United States, 385 U.S. 323, 341 (1966) (Douglas, J., dissenting); *see also* United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring) ("Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse."); *Ciraolo*, 476 U.S. at 225 n.10 (1986) (Powell, J., dissenting) ("It would appear that, after today, families can expect to be free of official surveillance only when they retreat behind the walls of their homes."); United States v. U.S. Dist. Court, 407 U.S. 297, 320 (1972) ("Official surveillance . . . risks infringement of constitutionally protected privacy of speech. Security surveillances are especially sensitive because of the inherent vagueness of the domestic security concept, the necessarily broad and continuing nature of intelligence gathering, and the temptation to utilize such surveillances to oversee political dissent."); *Johnson*, 333 U.S. at 14 ("The right of officers to thrust themselves into a home is also a grave concern, not only to the individual but to a society which chooses to dwell in reasonable security and freedom from surveillance."); *cf.* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 196 (1890) ("The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual.").

35. JAMES C. SCOTT, WEAPONS OF THE WEAK 36 (1985).

to block surveillance.[36] A focus solely on the legal victories of organized groups committed to limiting governmental overreaching may serve to downplay the importance of individual actions.[37] The focus of this Article is the following: How do ordinary people resist surveillance, and how should it influence our understanding of policing?

This Article aims to document privacy protests and to discuss why the police and courts should not ignore them.[38] Part I begins by identifying seemingly disparate acts that can be grouped together as privacy protests. Part II describes how these privacy protests have little salience either in police assessments of suspicious behavior or in judicial assessments of Fourth Amendment law. Part III demonstrates that despite this inattention, privacy protests have potential social value that counsels careful governmental responses. These individual actions demonstrate that the boundaries of privacy and legitimate governmental action are the product of a dynamic process. A more comprehensive account of privacy must consider not only the attempts of individuals to exert control over their own information, lives, and personal spaces, but also the ways in which they take active countermeasures against the government (and private actors[39]) to thwart attempts at surveillance.

I. WHAT ARE PRIVACY PROTESTS?

There are many ways to avoid, block, or deny police attempts to gain access to your personal information. Criminals too, will often take the very same steps to avoid discovery of their criminal wrongdoing. In many cases, the steps a person takes when she believes she is being surveilled look the same whether she is a criminal or an opponent of overzealous government surveillance. Relying heavily on prepaid cellphones, for instance, can serve different purposes: to avoid discovery of criminal activity or to thumb your nose at the police.

---

36. Marx also distinguishes individual efforts from collective ones in his own work. *See* Marx, *supra* note 24, at 271–72.

37. *See* LYON, *supra* note 1, at 178.

38. The central concern of this Article is the consideration of privacy protests under the Fourth Amendment. To the extent that such conduct might be considered "speech," it seems unlikely under current Supreme Court doctrine that the First Amendment poses any doctrinal obstacles to police action. *See, e.g.*, United States v. O'Brien, 391 U.S. 367, 376 (1968) (rejecting the "view that an apparently limitless variety of conduct can be labeled 'speech' whenever the person engaging in the conduct intends thereby to express an idea"); *see also* Wisconsin v. Mitchell, 508 U.S. 476 (1993). And while this Article focuses particularly on Fourth Amendment law, the recognition of privacy protests likely has implications for other areas of the law, such as civil suits for unauthorized computer use and access. *See, e.g.*, DirecTV, Inc. v. Borow, No. 03 C 2581, 2005 WL 43261, at *6 (N.D. Ill. Jan. 6, 2005) (permitting adverse inference against defendant based on his use of evidence eliminator software).

39. Some of these people will act in ways to thwart surveillance of any kind, whether the source is public or private. *See generally* Marx, *supra* note 24, at 375–77. Although objections to surveillance by private actors are equally worthy of examination, they lie beyond the scope of this discussion because they do not raise the same Fourth Amendment concerns.

Some of these techniques are simple and relatively inexpensive, such as wearing a disguise, staying in constant movement, and speaking in secluded places. Other methods, however, rely on increasingly sophisticated and inexpensive technologies available for purchase, either in the legitimate consumer marketplace or in black markets. Some private detectives have reversed their traditional role as trackers by helping people erase their digital "footprints" on the internet and in electronic records by creating multiple identities, generating false electronic documents, and wiping out truthful information.[40] Consumers can also buy computer software such as Evidence Eliminator to "wipe" computer hard drives[41] and counter-surveillance programs to find out if someone is monitoring their computer.[42]

Of course, some steps individuals take are so extreme or so expensive that they are unlikely to represent only a privacy protest. Just as the possession of burglar's tools can point to little else but the likelihood of a past or planned crime, some actions have little noncriminal value.[43] Expense is a factor. The fabrication of genetic information is likely expensive enough to discourage widespread consumer use, at least for now.[44] Changing small details of one's records on the

---

40. Services such as Web 2.0 Suicide Machine promise to purge your data from online social networks. *See* Sophia Yan, *How to Disappear from Facebook and Twitter*, TIME (Jan. 19, 2010), http://content.time.com/time/business/article/0,8599,1954631,00.html. In the case of Web 2.0 Suicide Machine, however, Facebook banned the company's IP address from accessing Facebook accounts. *See* David Colker, *Facebook Fights Back, Disallows the Suicide Machine*, L.A. TIMES BLOG (Jan. 4, 2010, 6:15 AM), http://latimesblogs.latimes.com/technology/2010/01/facebook-fights-back-disallows-the-suicide-machine.html.

41. *See, e.g.*, Eric A. Taub, *Deleting May Be Easy, but Your Hard Drive Still Tells All*, N.Y. TIMES, Apr. 5, 2006, at G4 (noting that overwriting software is "popular" but can "draw a red flag in legal circles").

42. *See, e.g.*, Jennifer Leighton, *How to Find Keyloggers & Malware on a Laptop*, OPPOSING VIEWS, http://science.opposingviews.com/keyloggers-malware-laptop-9268.html (last visited Oct. 6, 2013).

43. For this reason, many states criminalize the possession of burglar's tools. As the late William Stuntz pointed out, however, such crimes provide prosecutors with shortcuts, but they do a poor job of identifying actual burglars. Many of these statutes amount to "bans on possessing screwdrivers, perhaps with an implicit additional term requiring that the possession seem suspicious." William Stuntz, *The Pathological Politics of Criminal Law*, 100 MICH. L. REV. 505, 516 n.50 (2001). Even this may not be an unqualified act of criminal intent: Lock picking has become a noncriminal hobby, particularly within the "hacker" community. *See* Paul Rubens, *Hackers Turn to Lock Picking for Sport*, BBC NEWS (July 20, 2010), http://www.bbc.co.uk/news/technology-10554538.

44. In 2009, a life sciences company in Israel demonstrated that it is possible to fabricate DNA evidence. The lead author of the paper discussing these findings stated, "You can just engineer a crime scene." Andrew Pollack, *Scientists Show That It's Possible to Fake DNA Evidence*, N.Y. TIMES, Aug. 18, 2009, at D3. While the process, according to the company's founder, could be completed by a "biology undergraduate," it does require the laboratory equipment necessary for genome amplification. Katherine Harmon, *Lab Creates Fake DNA Evidence,* SCI. AM. (Aug. 18, 2009), http://www.scientificamerican.com/blog/post.cfm?id=lab-creates-fake-dna-evidence-2009-08-18.

internet may require modest expense and effort, but the creation of an entire virtual identity, accompanied by the real world creation of an alternate address and bank account and the deliberate use of a credit card in several locations, is likely to be undertaken only by someone who does not wish to be found under any circumstances.[45] Criminals may be the only people who elect to undergo identity-changing plastic surgery, but there are matters of degree. Asking a surgeon to graft skin from another part of the body to one's fingertips is likely the act of a fugitive;[46] applying superglue to one's fingertips may not be.[47]

Apart from these extreme examples, individuals take numerous steps to shield their actions from the government even though they are not engaged in any criminal activity. Despite innocent intentions, privacy protests often suggest to the police that individuals are behaving in criminally suspicious ways, because most of these actions are indistinguishable from steps criminals often take.

No matter what their level of sophistication, privacy protests can be categorized into several types. Sociologist Gary Marx classifies several ways in which people deliberately avoid surveillance.[48] The sections that follow define several important categories of such surveillance evasions and provide examples of their criminal and noncriminal uses.

A. Discovery Moves

Some people simply want to find out whether the police are watching them and what the nature of that surveillance is.[49] A simple technique exploiting the presence of cyanoacrylate, a chemical in Super Glue, can detect the presence of another person's fingerprints on places where fingerprinting dust cannot.[50]

---

45. A criminal or an individual who fears being traced by someone who poses a threat, such as an abusive spouse, may take such steps. *See* AHEARN & HORAN, *supra* note 18, at 71–74.

46. *Cf.* Michael Powell, *Tips for the Sophisticated Fugitive*, N.Y. TIMES, Mar. 22, 2009, at WKS5 (describing options for fugitives including "[a] touch of plastic surgery and a discreet payoff" in a place with no extradition treaty).

47. *See, e.g.*, Mimi Hall, *Criminals Go to Extremes to Hide Identities*, USA TODAY (Nov. 6, 2007, 1:41 AM), http://usatoday30.usatoday.com/news/nation/2007-11-06-criminal-extreme_N.htm (describing criminals who have applied superglue or burned their fingertips to hide their fingerprints).

48. *See* Marx, *supra* note 24, at 274.

49. *Id.* at 274–75.

50. *See, e.g.*, Eric W. Brown, *The Cyanocrylate Fuming Method*, http://www.ccs.neu.edu/home/feneric/cyanoacrylate.html (last visited Nov., 2, 2013) (describing technique and efficacy of Super Glue method); *Super-Glue Fingerprints Activity*, STAPLES HIGH SCHOOL FORENSICS, http://shs2.westport.k12.ct.us/forensics/04-fingerprints/super-glue.htm (suggesting elementary school activity to detect fingerprints with Super Glue).

Surveillance cameras and GPS detectors can reveal the presence of human or electronic eavesdroppers.[51]

Those engaged in privacy protests might also borrow techniques from the criminal world to test the motivations of friends, neighbors, or business associates. Criminals necessarily rely upon discovery moves to distinguish real criminal associates and potential customers (drug users, johns, and the like) from phonies. The demand for "criminal credentials" usually requires that a person commit a crime.[52] In a criminal organization such as La Cosa Nostra, a would-be member's willingness to "make his bones" (i.e., kill someone) to become a "made guy" is required in part to reveal the presence of undercover police.[53] A longstanding technique used by street drug sellers is a demand that a suspect buyer consume some of the product before the sale.[54] Here, the assumption the seller makes is that an undercover agent would not consume illegal drugs; police officers are typically prohibited from ingesting drugs except in life threatening emergencies.[55] To counter this counter-surveillance technique, many undercover officers have developed strategies either to feign drug use or to present credible stories that explain their inability to "test" the goods.[56] Borrowing from these techniques, one might choose to question an unfamiliar social contact extensively before revealing any personal information.

B. Avoidance Moves

If I discover that I am the target of surveillance, I may seek to avoid it by moving in time and space to places where the surveillance is absent or is unlikely to find me.[57] At one time, the constant switching of meeting places, safe houses, and pay phones might have sufficed to protect privacy. Today, however, surveillance targets often need to avoid specific technologies that are easily capable of tracking, such as cell phones,[58] electronic toll responders,[59] and retail

---

51. *See, e.g.*, *Check Your Car for a GPS Tracker*, WIRED, http://howto.wired.com/wiki/Check_Your_Car_for_a_GPS_Tracker (last modified May 14, 2011, 12:42 AM).

52. DIEGO GAMBETTA, CODES OF THE UNDERWORLD: HOW CRIMINALS COMMUNICATE 9–10 (2009).

53. *See id.* at 17–19, 23–24.

54. *See, e.g.*, Elizabeth E. Joh, *Breaking the Law to Enforce It: Undercover Police Participation in Crime*, 62 STAN. L. REV. 155, 166–67 (2009) (discussing how criminals use this and similar techniques to flush out undercover police agents).

55. *See, e.g.*, David Kocieniewski, *In New York City Drug War, Risky Tactics and Casualties*, N.Y. TIMES (Jan. 21, 1998), http://www.nytimes.com/1998/01/21/nyregion/in-new-york-city-drug-war-risky-tactics-and-casualties.html?pagewanted=1 (describing this policy for undercover work in the NYPD).

56. *See, e.g.*, Bruce A. Jacobs, *Undercover Drug-Use Evasion Tactics: Excuses and Neutralization*, 15 SYMBOLIC INTERACTION 435, 447–48 (1992).

57. *See* Marx, *supra* note 24, at 374–77.

58. Eric Lichtblau, *Police Are Using Phone Tracking as a Routine Tool*, N.Y. TIMES, Apr. 1, 2012, at A1 (describing "hundreds" of police departments' use of cell phone tracking, often with no judicial oversight).

loyalty shopper cards.[60] Such technologies can pinpoint a person's precise location in time and space. These avoidance moves can sometimes backfire, however, and draw police attention. For instance, prepaid cellphones, or "burners," are favorites of drug dealers and political activists because they require no identification for purchase.[61] Yet large purchases of prepaid cell phones have also aroused police suspicions that the users were involved in terrorist planning activities.[62]

C. Blocking Moves

If avoidance moves are passive, those engaged in masking or blocking moves take more active steps both to signal that they are aware of the surveillance as well as to avoid detection.[63] In blocking moves, the surveillance target tries to prevent access to the information the police seek.[64] For example, criminals often resort to blocking moves. A common scene from bank heist films involves thieves donning women's pantyhose to obscure their features. Professional shoplifting rings use booster bags lined with foil or duct tape to block anti-theft scanners from detecting stolen merchandise.[65]

Similarly, privacy protests can be used to block police surveillance. Consider facial recognition software of the sort the Tampa police used at the 2001 Superbowl to identify terrorists and felons.[66] Such software relies heavily on the

---

59. *See, e.g.*, Madison Park, *E-ZPass Details Popping Up in Trials*, BALTIMORE SUN (Aug. 31, 2007), http://articles.baltimoresun.com/2007-08-31/news/0708310082_1_zpass-toll-records-electronic-toll (describing prosecutors' increasing use of E-ZPass records); Deborah Mcdermott, *EZPass Transponder Records Used in Dodds Case*, SEACOASTONLINE (Feb. 5, 2008, 2:30 PM), http://www.seacoastonline.com/articles/20080205-NEWS-80205050 (describing prosecutors' use of electronic toll responder records to refute defendant's account of his whereabouts).

60. *See, e.g.*, *Firefighter Arrested for Attempted Arson*, KOMONEWS (Aug. 28, 2004, 8:30 PM), http://www.komonews.com/news/archive/4132241.html (reporting arrest of man on suspicion of arson after police detectives found evidence of fire starter purchase through his grocery loyalty card).

61. Peter Maass & Megha Rajagopalan, *That's No Phone. That's My Tracker*, N.Y. TIMES, July 15, 2012, at 5.

62. *See* Brian Ross & Richard Esposito, *Surge in Sale of Disposable Cell Phones May Have Terror Link*, ABC NEWS (Jan. 12, 2006), http://abcnews.go.com/WNT/Investigation/story?id=1499905 (describing FBI investigation into Middle Eastern and Pakistani persons' large purchases of prepaid cell phones in Texas and California). The anonymity of prepaid cell phones—which does not require formal identification or a credit card—may soon be gone. *See* Jim Dwyer, *It's Not Just Drug Dealers Who Buy Prepaid Phones*, N.Y. TIMES, May 30, 2010, at MB1 (describing legislation that Senators Charles Schumer and John Cornyn sponsored that would require purchasers to provide identification).

63. *See* Marx, *supra* note 24, at 379–81.

64. *See id.*, at 379.

65. *See, e.g.*, John Colapinto, *Stop, Thief: The High-Tech Approach to Catching Shoplifters*, THE NEW YORKER, Sept. 1, 2008, at 74.

66. *See* Declan McCullagh, *Call It Super Bowl Face Scan I*, WIRED (Feb. 2, 2001), http://www.wired.com/politics/law/news/2001/02/41571 (reporting that facial recognition software secretly scanned every person who passed through the turnstiles and attempted to match their faces with known criminal mugshots).

measurements around the eyes and nose,[67] but has its limitations. Artist Adam Harvey, who has drawn attention for his products designed to thwart surveillance technology,[68] discovered that dramatic facial makeup thwarts facial recognition software.[69] Thus, attempts to create an "anti-face" with makeup confuse the computer algorithms powering such software and render them useless.[70]

Faces that cannot be detected with facial recognition software.[71]

Many blocking moves are available to anyone through the use of cheap and legal technologies. An inexpensive laser pointer can disable a surveillance camera.[72] A thirty-dollar device bought over the internet can jam GPS signals so they cannot be tracked.[73] Blocking films frustrate license plate readers.[74] Companies like Silent Circle have developed technologies to permit "surveillance-

67. Jesse Emspak, *How to Beat Facial Recognition Software*, NBC NEWS, http://www.nbcnews.com/id/46153896/ns/technology_and_science-security/#.Un-nPPnYeSo (last updated Jan. 26, 2012, 4:49 PM) (reporting that the "critical region" for facial recognition technology is "the space around the bridge of the nose and between the eyes").

68. *See, e.g.*, Ryan Gallagher, *The Anti-Surveillance Clothing Line that Promises to Thwart Cell Tracking and Drones*, SLATE (Jan. 11, 2013, 2:57 PM), http://www.slate.com/blogs/future_tense/2013/01/11/stealth_wear_adam_harvey_s_clothing_line_safeguards_against_surveillance.html.

69. Emspak, *supra* note 67.

70. *See* John D. Sutter, *How to Hide from Face-Detection Technology*, CNN (Apr. 29, 2012, 10:25 AM), http://whatsnext.blogs.cnn.com/2012/04/29/how-to-hide-from-face-detection-technology/ (describing CV Dazzle, Harvey's project).

71. Dan Goodin, *Reverse-Engineering Artist Busts Face Detection Tech*, THE REGISTER (Apr. 22, 2010), http://www.theregister.co.uk/2010/04/22/face_detection_hacking/ (showing pictures that thwart Viola-Jones algorithm used in facial recognition technology).

72. John Markoff, *Protesting the Big Brother Lens, Little Brother Turns an Eye Blind*, N.Y. TIMES, Oct. 7, 2002, at C1 (describing efforts of Michael Naimark to disable surveillance cameras in public with inexpensive laser pointer and to share his instructions on the internet).

73. Although GPS jammers are illegal in the United States, they are inexpensive and widely available for purchase on the internet. *See, e.g.*, David Hambling, *GPS Signals Now Help You Call Your Mother, Power Your Home, and Even Land Your Plane…But a Cheap Plastic Box Can Jam it All*, NEW SCIENTIST, March 12, 2011, at 44 (describing how such jammers can wreak havoc on a variety of everyday activities such as cellphone communications, electricity grids, and stock exchanges).

74. Oldenburg, *supra* note 16, at A01.

resistant" communications on mobile devices.[75] One day it may be possible to mask conversations with "audio cloaks" that generate digital "noise," or to prevent unwanted photography by wearing jewelry with infrared light that blurs pictures taken in one's direction.[76]

D. Masking Moves

A masking move goes further than blocking access to the sought information by presenting false or misleading clues such as manufactured social security numbers, identities, or license plates. Both blocking and masking moves may prevent the police from retrieving authentic information (such as names, serial numbers, or addresses), but masking moves are intended to deceive the police.[77] In some cases, the police may not realize that they have been misled.

A voice distortion device changes the quality and pitch of a caller's voice.[78] A GPS "spoofer" can provide misleading data about location; for instance, a fishing boat captain could use such a device to hide his location in illegal fishing waters.[79] A virtual phone number with no physical location, or a misleading one, makes it nearly impossible to find out the caller's location.[80] The purposeful addition of small errors in the spelling of one's name and address in online records can make internet tracking more difficult.[81] In the futuristic film *The Minority Report*, the main character undergoes black market eye replacement surgery to avoid being hunted down in a world where optical recognition machines pervade ordinary life.[82] In real life, fugitives may don wigs, odd clothes, makeup, and, in some extreme cases, may undergo plastic surgery.[83] Fabricated DNA might one day be used to mask one's genetic traces.[84]

---

75. Ryan Gallagher, *New "Surveillance-Proof" App to Secure Communications Has Governments Nervous*, SLATE (Oct. 16, 2012, 6:00 PM), http://www.slate.com/articles/technology/future_tense/2012/10/silent_circle_mike_janke_s_iphone_app_makes_encryption_easy_governments.single.html.

76. Bilton, *supra* note 2, at B5.

77. *See* Marx, *supra* note 24, at 380.

78. *See* William Grimes, *High-Tech Talk*, N.Y. TIMES (Apr. 4, 1993), http://www.nytimes.com/1993/04/04/magazine/high-tech-talk.html (describing the operation of the Questech International Transition 2000, a "voice changing telephone").

79. *See* Hambling, *supra* note 73, at 44 (reporting that spoofers are not yet on the market but that the technology is already available).

80. *See* AHEARN & HORAN, *supra* note 18, at 83–84.

81. *See id.* at 53–61 (advising how to engage in "misinformation").

82. THE MINORITY REPORT (DreamWorks 2002).

83. *See* Joan Kron, *Only His Surgeon Knows for Sure*, N.Y. TIMES (Feb. 17, 1999), http://www.nytimes.com/1999/02/17/health/only-his-surgeon-knows-for-sure.html?pagewanted=all&src=pm ("Fugitives have become a niche market in plastic surgery: drug dealers, gangsters, terrorists, political refugees, spies and witnesses under government protection.").

84. *See* Dan Frumkin & Adam Wasserstrom, *Authentication of Forensic DNA Samples*, 4 FORENSIC SCI. INT'L: GENETICS 95, 102–03 (2010) (demonstrating the "ease" with which artificial DNA can be produced and potentially passed off as real samples in

E. Why People Avoid Surveillance

What distinguishes privacy protests from the evasive steps criminals take are the intentions behind such protests. In addition, privacy protests have at least the potential to be socially useful. While a criminal's motives are generally unsympathetic, a person engaged in a privacy protest may have motives that resonate with those who identify themselves as civil libertarians, critics of "big" government, and even anarchists, although the protester may not formally align herself with any particular group.

Because the perceived threats are not easily identifiable, the reasons for some of these protests will be difficult to distinguish from one another. Some will evade perceived government surveillance, not because they object to a single act of surveillance, but rather to protest the hundreds of pieces of data collected about them that provide, when assembled, a "digital dossier" about their lives.[85] Complicating matters further is the fact that the data police use may be initially collected by private entities that sell and share information to other parties for a profit.[86] Yet other individuals object to the growing presence of surveillance in their lives no matter whether it comes from public or private entities. The use of a disposable email address might be an objection both to private corporations that track consumers as well as to the government.

Privacy protestors engage in these acts even though they require extra effort. Burner phones, for example, protect privacy, but they are also cumbersome to use when compared to phones connected to larger service providers.[87] Using prepaid credit cards requires extra effort as well.[88] In fact, privacy protestors may resort to the same consumer products as the poor who have no choice but to use prepaid phone and cash. Privacy, like poverty, has its own costs.[89]

---

crime scenes); Pollack, *supra* note 44 (suggesting that fabricated genetic evidence could be planted at a crime scene).

85. *See* Dan Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1084 (2002).

86. *See, e.g.*, Chris Jay Hoofnagle, *Big Brother's Little Helpers: How Choicepoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C. J. INT'L L. & COM. REG. 595, 598–622 (2004) (discussing privacy concerns raised by government access to commercial data brokers' information).

87. *See The Pros and Cons of a Prepaid Cell Phone*, TIMES UNION (Dec. 21, 2012, 3:54 PM), http://www.timesunion.com/business/article/The-Pros-and-Cons-of-a-Prepaid-Cell-Phone-4158058.php.

88. *See, e.g.*, Susan Johnston, *The Perils of Prepaid Debit Cards*, U.S. NEWS & WORLD REPORT (Jan. 22, 2013), http://money.usnews.com/money/personal-finance/articles/2013/01/22/the-perils-of-prepaid-debit-cards (discussing hidden costs of using prepaid cards compared to conventional credit cards).

89. Thanks to Christopher Soghoian for this observation. *See also* DeNeen L. Brown, *Poor? Pay Up,* WASH. POST (May 18, 2009), http://articles.washingtonpost.com/2009-05-18/news/36823675_1_poverty-line-middle-class-milk (describing various costs low income people suffer as a direct result of their poverty).

Not all privacy protests represent a strike against technology. When a neighbor draws his blinds or burns his garbage, he is resisting surveillance.[90] In some cases, privacy protests originate out of racial or ethnic tensions. Arab-Americans in Detroit or African-Americans in the South Bronx may engage in privacy protests because they feel police have intruded needlessly into the private lives of others in their communities, even if they have not been affected personally.[91]

Yet what is not generally recognized is that these protests—whether originating from the online community or urban ones—are structurally similar. This has two consequences: 1) Both types of protests should be treated similarly and 2) These groups have a common interest that could spur collective action.

II. PRIVACY PROTESTS AND CRIMINAL SUSPICION

As the previous Section explained, privacy protests and criminal secrecy may appear superficially similar, but they are distinct in important respects. The problem with this apparent similarity is that both kinds of evasion can attract police suspicion, and suspicion is a central facet of the police officer's world view.

A. The Central Role of Suspicion

Sociologists and reporters who have spent hours in patrol cars with police can attest to one thing: Ordinary patrol work consists of long stretches of boredom punctuated with the occasional burst of excitement, and even more rarely, real violence.[92] The introduction of the two-way radio and the police cruiser not only revolutionized patrol work, it also resulted in the common practice of a single officer cruising around streets while listening in for calls from central dispatch.[93] While crime fighting might be central to the self-image of the police,[94] actual policing is very much a service job catering to decidedly less glamorous problems, such as the drunk and disorderly, family disputes, and lost children.[95] Yet police

---

90. *See* LYON, *supra* note 1, at 166.

91. Criminal procedure scholars have pointed out that the perception of racially biased policing can lead to a lack of trust in the police and noncompliance with the law. *See, e.g.*, Erik Luna, *Transparent Policing*, 85 IOWA L. REV. 1107, 1160–63 (2000). Another possible consequence is an increase in privacy protests.

92. *See, e.g.*, RICHARD V. ERICSON, REPRODUCING ORDER: A STUDY OF POLICE PATROL WORK 206 (1982) (observing that "the bulk of the patrol officer's time was spent doing nothing other than consuming the petrochemical energy required to run an automobile and the psychic energy required to deal with the boredom of it all").

93. *See, e.g.*, Albert J. Reiss, Jr., *Police Organization in the Twentieth Century*, 15 CRIME & JUST. 51, 58 (1992) (discussing importance of technological change to modern policing).

94. *See, e.g.*, John Van Maanen, *Observations on the Making of Policemen*, 32 HUMAN ORG. 407, 414 (1973) (noting "patrolman's self-image of performing a worthwhile, exciting, and dangerous task" in contrast to the realities of the job).

95. *See, e.g.*, *id*. (observing that "a patrolman is predominantly an order taker—a reactive member of a service organization").

work is not only reactive. Investigating suspicious behavior is an equally important tool of policing.

Police officers depend upon their personal judgment of suspicious behavior: an innately fuzzy, intuitive, and ill-defined concept. To be sure, the modern police department's crime fighting arsenal includes crime mapping, statistical analysis, and other quantitative data, but hunches—quick judgments about suspicious behavior—remain significant.[96] In his famous 1960s study of the Oakland, California police, sociologist Jerome Skolnick observed that the "working personality" of the patrol officer can be characterized by a general suspiciousness.[97] That suspiciousness is premised upon a sense of what is normal[98]: a set of conditions based on a familiarity with the community, interactions with the public, and the collective knowledge of fellow officers. Little has changed about this basic aspect of the police officer's occupational identity.[99]

B. Police Suspicion and the Fourth Amendment

Constitutional law constrains how the police may act upon those suspicions. In order to comply with the Fourth Amendment, the police must justify their reason for interfering with a person's liberty. The Supreme Court's Fourth Amendment decisions, however, have not regulated police suspicion very restrictively.[100] For more than forty years, the Court has issued decisions that have both departed from the Fourth Amendment's literal probable cause requirement as well as sanctioned lesser degrees of police suspicion that permit interference with individual privacy.[101]

The Court's decisions do not provide much practical guidance on the circumstances in which one can evade police surveillance without drawing the kind of suspicion that results in unwanted police questioning or pursuit. While the

---

96. Craig Lerner helpfully defines a hunch as a quickly formed judgment that is neither easily articulated by the person coming up with the hunch nor is experienced as a "reasoned" judgment. Craig S. Lerner, *An Introduction to Police Hunches*, 4 J.L. ECON. & POL'Y 1, 3–4 (2007).

97. JEROME H. SKOLNICK, JUSTICE WITHOUT TRIAL 44 (1966) (observing that an officer is "generally a 'suspicious' person" because of the elements of danger and authority that shape his work).

98. *See id.* at 48 ("Policemen are indeed specifically *trained* to be suspicious, to perceive events or changes in the physical surroundings that indicate the occurrence or probability of disorder.").

99. To a certain extent, stereotyping is a feature of many professions. *See e.g.,* Andrew E. Taslitz, *Police Are People Too: Cognitive Obstacles to, and Opportunities for, Police Getting the Individualized Suspicion Judgment Right*, 8 OHIO ST. J. CRIM. L. 7, 48 (2010) ("[T]he police, like many professionals, are likely over time to see categories of cases rather than unique individuals or situations.").

100. *See, e.g.*, Lerner, *supra* note 96, at 7 (observing that current legal rules amount to little more than a "pleading requirement" where the police "regularly stop people on little more than a hunch, but simply shape what they say, months later, when they appear in court").

101. *See, e.g.*, Terry v. Ohio, 392 U.S. 1 (1968) (permitting search and seizure premised upon less than probable cause).

Court has required that an officer have more than an "inarticulate hunch[]"[102] before restraining a person's freedom of movement, it has refrained from demanding a checklist or a set of quantifiable factors for a constitutionally acceptable basis of suspicion.[103] The Court has even permitted the police to use factors that are just as consistent with innocent as with criminal behavior.[104] Yet the Court has also recognized that the refusal to cooperate with the police, without more, fails to provide any required suspicion for further investigation,[105] and that people are free to walk away from the police or refuse to answer questions without fear of being detained.[106]

Nonetheless, an avoidance move in a bad neighborhood can get you in trouble. In the late morning of September 9, 1995, Officer Timothy Nolan and his partner were assigned with six other Chicago Police Department officers to patrol the Eleventh District.[107] Nolan and the others drove by Sam Wardlow, who was standing on the street. When Wardlow saw the officers, he fled down an alleyway. The flight prompted Nolan to pursue Wardlow in his cruiser. Upon stopping and patting Wardlow down, Nolan found a .38 caliber handgun and five rounds of ammunition, and placed him under arrest for illegal firearms possession.[108] Nolan later testified that he and his fellow officers were driving in the area because the

---

102. *Id.* at 22.

103. *See, e.g.*, Ornelas v. United States, 517 U.S. 690, 696 (1996) (noting that probable cause and reasonable suspicion are "fluid concepts that take their substantive content from the particular contexts in which the standards are being assessed"); Illinois v. Gates, 462 U.S. 213, 232 (1983) (stating that probable cause is "not readily, or even usefully, reduced to a neat set of legal rules"); United States v. Cortez, 449 U.S. 411, 418 (1981) ("Long before the law of probabilities was articulated as such, practical people formulated certain common sense conclusions about human behavior; jurors as factfinders are permitted to do the same—and so are law enforcement officers."); Brinegar v. United States, 338 U.S. 160, 175 (1949) (noting that probable cause "deal[s] with probabilities . . . [that are] not technical; they are the factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act").

104. *See, e.g.*, Illinois v. Wardlow, 528 U.S. 119, 126 (2000) ("*Terry* [*v. Ohio*] accepts the risk that officers may stop innocent people. Indeed, the Fourth Amendment accepts that risk in connection with more drastic police action; persons arrested and detained on probable cause to believe they have committed a crime may turn out to be innocent."); *cf.* United States v. Arvizu, 534 U.S. 266, 277 (2002) ("[R]easonable suspicion . . . need not rule out the possibility of innocent conduct.").

105. *See, e.g.*, Florida v. Bostick, 501 U.S. 429, 437 (1991) (noting that a person's "refusal to cooperate, without more, does not furnish the minimal level of objective justification needed for a detention or seizure"); *see also Terry*, 392 U.S. at 34 (White, J., concurring) (noting that where the police lack reasonable suspicion, "the person approached may not be detained or frisked but may refuse to cooperate and go on his way").

106. *See, e.g.*, United States v. Margeson, 259 F. Supp. 256, 265 (E.D. Pa. 1966) ("[F]light, in and of itself, is not sufficient to constitute probable cause for otherwise anyone, who does not desire to talk to the police and who either walks or runs away from them would always be subject to a legal arrest."); *see also* United States v. Sharpe, 470 U.S. 675, 707 (1985) (Brennan, J., dissenting).

107. *Wardlow*, 528 U.S. at 121.

108. *Id.* at 122.

Eleventh District was notorious for its illegal drug trade.[109] The Eleventh District was, and continues to be, a section of Chicago that is plagued by violent crime and illegal drug sales.[110]

The Supreme Court ultimately upheld Nolan's decision to detain and frisk Wardlow. Two factors were critical to supporting Nolan's determination that he had the required reasonable suspicion: the fact that Wardlow was in the Eleventh District—a "high crime neighborhood"—and his "unprovoked flight" from the police.[111] Prior to *Illinois v. Wardlow*, a number of lower courts had questioned whether evading police surveillance could ever constitute a permissible factor in an officer's decision to detain anyone.[112] Citing that "dislike of authority" can be a legitimate concern, some lower courts had explicitly rejected avoidance of the police as a basis for reasonable suspicion.[113] Other lower court decisions, however, had held that evasive actions by themselves may justify a *Terry* stop.[114] The Supreme Court, however, found that Wardlow's decision to run was, if not strong evidence of wrongdoing, at least "certainly suggestive of such."[115]

Because it was his flight from the police that prompted police suspicion, Wardlow's case is not only a story about drug interdiction in a rough Chicago neighborhood, but also, when understood broadly, an illustration of a privacy protest. Sam Wardlow did in fact have something to hide, of course, and that occasioned his flight. Yet before Nolan discovered his handgun, Wardlow prompted suspicion because of his avoidance move, an act that is as consistent

---

109. People v. Wardlow, 701 N.E.2d 484, 485 (Ill. 1998), *rev'd*, 528 U.S. 119 (2000).

110. *See, e.g.*, Chuck Goudie, *Intelligence Report: 7-11 Initiative Targets Crime in Chicago's Most Violent Districts*, ABC 7 NEWS (June 13, 2012), http://abclocal.go.com/wls/story?section=news/iteam&id=8700287 (noting that the 7th and 11th districts of Chicago produce a quarter of the violent crime in the city).

111. *Wardlow*, 528 U.S. at 124.

112. *See, e.g.*, *Wardlow*, 701 N.E.2d at 486 (collecting cases), *rev'd*, 528 U.S. 119 (2000).

113. *See, e.g.*, State v. Hicks, 488 N.W.2d 359, 364 (Neb. 1992) ("Fear or dislike of authority, distaste for police officers based upon past experience, exaggerated fears of police brutality or harassment, and fear of unjust arrest are all legitimate motivations for avoiding the police.").

114. *See, e.g.*, State v. Anderson, 454 N.W.2d 763, 766 (Wis. 1990) ("Flight at the sight of police is undeniably suspicious behavior. Although many innocent explanations could be hypothesized as the reason for the flight, a reasonable police officer who is charged with enforcing the law as well as maintaining peace and order cannot ignore the inference that criminal activity may well be afoot."). A problem that has emerged since *Wardlow* is whether the avoidance of a checkpoint by itself justifies a *Terry* stop. *See, e.g.*, Shan Patel, *Per Se Reasonable Suspicion: Police Authority to Stop Those Who Flee from Road Checkpoints*, 56 DUKE L.J. 1621, 1638–39 (2007) (noting that lower courts disagree as to whether such evasion constitutes reasonable suspicion).

115. *Wardlow*, 528 U.S. at 124.

with a privacy protest as with criminality.[116] That evasion, coupled with his location, granted the police a license to stop and tackle Wardlow.

The Supreme Court has, on many occasions, acknowledged that Fourth Amendment decisions may sometimes lead to the detention of innocent people.[117] These mistakes are explained as necessary risks that accompany police work.[118] Those engaged in privacy protests, however, are not merely innocents who are caught up inadvertently in police investigations. They may deliberately engage in tactics that may pique police suspicion, although they have engaged in no criminal activity. Fourth Amendment law[119] provides little basis to distinguish between behavior that legitimately invites police suspicion and that which should be left alone because it might protest the surveillance itself.[120]

C. The Problem with Police Suspicion

While police rely heavily on their own identification of suspicious behavior, these judgments are not a particularly sophisticated tool for ferreting out criminal wrongdoing. Because suspicious behavior is often unusual behavior, police judgments about criminally suspicious behavior are necessarily hunches about abnormality, regularity, and conformity.[121]

---

116. When viewed this way, the "unprovoked flight" may have social value, at least at the time the suspicion is formed. *Contra* Atkinson, *supra* note 100, at 1562 (arguing that Wardlow's flight "seems unlikely to have a large social value").

117. *See, e.g.*, *Wardlow*, 528 U.S. at 126 ("In allowing . . . detentions, *Terry* accepts the risk that officers may stop innocent people."); United States v. Sokolow, 490 U.S. 1, 9 (1989) (noting that factors consistent with criminal activity are commonly "quite consistent with innocent [behavior]").

118. *See Wardlow*, 528 U.S. at 126.

119. In considering the Fifth Amendment privilege against self-incrimination, some lower courts have had to determine whether criminal suspects must submit passwords to the government for encrypted files that are suspected of containing incriminating evidence. *See, e.g.*, *In re* Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1347 (11th Cir. 2012) (observing that the simple existence of encrypted files did not mean that the suspect "was trying to hide something[;] just as a vault is capable of storing mountains of incriminating documents, that alone does not mean that it contains incriminating documents, or anything at all"). Here, too, the possibility of privacy protests should be considered.

120. Indeed, as David Harris documented in an article dated before the *Wardlow* decision, lower courts were interpreting *Terry v. Ohio* so as to permit generalized police judgments that justified the stop and frisk of "almost anyone they want, with minimal interference from the courts." *See* David A. Harris, *Particularized Suspicion, Categorical Judgments: Supreme Court Rhetoric Versus Lower Court Reality Under* Terry v. Ohio, 72 ST. JOHN'S L. REV. 975, 977 (1998); *see also* Douglas H. Ginsburg, *Of Hunches and Mere Hunches: Two Cheers for* Terry, 4 J.L. ECON. & POL'Y 79, 86 (2007) (noting that "courts are . . . extremely reluctant to second-guess the decision of an experienced police officer—a repeat player in the game of catching criminals").

121. *See, e.g.*, SKOLNICK, *supra* note 97, at 48 (noting that a police officer's dominant characteristic is the "almost desperate love of the conventional" (quoting Colin McInnes, MR. LOVE AND JUSTICE 74 (1962))).

At best, an experienced police officer uses her knowledge of the neighborhood, past experience with criminals, and professional training to discern what is suspicious. Unless clearly unsubstantiated, the Supreme Court has been reluctant to second guess these judgments.[122] Although the Fourth Amendment requires the police to provide specific, individualized reasons for stops and arrests,[123] the likely truth is that even seasoned officers probably cannot articulate fully why a suspect stood out to them as criminally suspicious.[124]

Recent literature on the quickly made judgments of police officers and other professionals suggests that intuition can produce reliable judgments. As journalist Malcolm Gladwell discussed in his popular book *Blink*, quick and intuitive judgments can be as accurate as deliberate and cautiously made ones.[125] Certainly, many of the hunches police act upon will prove to be correct.

The problem, however, is that far too many hunches police act upon are inaccurate. Innocent persons can be detained or arrested as a result. While any process involving human decisionmaking will produce some errors, the results of problematic hunches in police work can be dramatic. For example, the overwhelming majority—eighty-eight percent—of the nearly 700,000 New Yorkers stopped in 2011 through the NYPD's aggressive stop-and-frisk policies were immediately released.[126] Many have argued that these stops of innocent persons can be attributed to racism on the part of the police.[127] While conscious racist attitudes might explain some of these unwarranted stops, they are unlikely to

---

122. *See* Elizabeth E. Joh, *Discretionless Policing: Technology and the Fourth Amendment*, 95 CAL. L. REV. 199, 211–14 (2007).

123. *See, e.g.*, Terry v. Ohio, 392 U.S. 1, 21 (1968) (holding that individualized suspicion is required to satisfy the Fourth Amendment's reasonable suspicion standard).

124. *See* Lerner, *supra* note 96, at 6 (contrasting police officers' informal reliance on "sixth sense" with suppression hearings, in which "[t]he entire language of intuitive thinking is excised from their vocabulary"); Dan Horan, *A Hunch, or the Whispered Voice of Experience?*, 4 J.L. ECON. & POL'Y 13, 16–17 (2007) (an LAPD sergeant who writes that the basis for identifying a particular drug courier "is difficult if not impossible to describe").

125. MALCOLM GLADWELL, BLINK 14 (2005).

126. *See* N.Y. CIVIL LIBERTIES UNION, NYPD STOP-AND-FRISK ACTIVITY IN 2011, at 17 (2012), http://www.nyclu.org/files/publications/NYCLU_2011_Stop-and-Frisk_Report .pdf. The NYPD has come under increasing pressure to reduce the number of persons these policies target. *See, e.g.*, Joseph Goldstein & Wendy Ruderman, *Police Stops in New York Drop by 34%*, N.Y. TIMES, Aug. 4, 2012, at A1 (noting that, perhaps in response to public pressure, the number of stop and frisks NYPD officers conducted declined in the second quarter of 2012 by more than a third compared to the previous quarter).

127. *See, e.g.*, Bob Herbert, Editorial, *Jim Crow Policing*, N.Y. TIMES, Feb. 2, 2010, at A27 (arguing that NYPD stop and frisk policies amount to "a despicable, racially oriented tool of harassment"). According to the NYCLU report, black and Latino men accounted for a 41.6% of stops in 2011, although they make up only 4.7% of the city's population. *See* N.Y. CIVIL LIBERTIES UNION, *supra* note 126, at 2.

explain most of them.[128] Instead, many of these erroneous judgments can probably be attributed to cognitive shortcuts that police officers use to make quick decisions about whether to continue investigations.[129] Some of these heuristics have special relevance in the context of privacy protests.

First, people often have erroneous first impressions because they believe the people they judge are roughly similar to them in beliefs, attitudes, and knowledge.[130] Police assumptions may be especially pernicious because their "working personalities" tend to be more politically and socially conservative than those of the general public, including those communities they police.[131] Many have pointed out that this disparity is especially dramatic in low-income minority neighborhoods, where police and members of the community have few shared attitudes or experiences.[132] Where people fear the police because friends or family members have been the victims of perceived harassment, understandable avoidance of the police can easily be—and often is—interpreted as consciousness of guilt.[133] Similarly, members of the "hacker" community often express strong skepticism about government and consequently place a high value on methods that protect privacy and promote digital anonymity.[134]

A second common cognitive error can be attributed to our reliance on a set of narratives to help us interpret the world.[135] The police, like the rest of us, rely upon these mental models as they assess actual circumstances to see if danger or criminality is present.[136] The more diverse the set of mental models an officer has in mind when interpreting data, the less likely the conclusion the officer reaches is going to be wrong.[137] Thus, the goal is not to eliminate the use of stock

---

128. *Cf.* William J. Stuntz, *Race, Class, and Drugs*, 98 COLUM. L. REV. 1795, 1798–99 (1998) (arguing that class rather than race differences account for disproportionate enforcement against minorities).

129. For an insightful discussion of how cognitive science research helps illuminate the problems of police hunches, see generally Taslitz, *supra* note 99, at 46 (2007) (noting that not all researchers agree on the role of heuristics in everyday life, but providing reasons to believe that police officers in particular likely rely upon them).

130. *See id.* at 21 (describing error of "egocentrism").

131. *See, e.g.*, SKOLNICK, *supra* note 97, at 44.

132. *See, e.g.*, Taslitz, *supra* note 99, at 22 ("Police from a sharply different cultural background in which the officer is one's friend may thus overemphasize flight, misconstruing its meaning by seeing an effort to flee to safety as an effort to elude capture.").

133. *See, e.g.*, Illinois v. Wardlow, 528 U.S. 119, 126–40 (2000) (Stevens, J., concurring in part, dissenting in part) (discussing reasons why innocent persons might flee from the police).

134. *See, e.g.*, Tim Jordan & Paul Taylor, *A Sociology of Hackers*, 46 SOC. REV. 757, 764–65 (1998) (noting that secrecy and anonymity are two key characteristics of hacker culture).

135. *See, e.g.*, Taslitz, *supra* note 99, at 38–39 (discussing how police interpretation of facts involves "sense making through storytelling").

136. *See id.*

137. *See id.*

stories, a likely impossible task, but rather to "help police build richer narrative mental models."[138]

The mental model that might have the most impact on privacy protests is one that assumes that "innocent people have nothing to hide."[139] The slogan the British government adopted to promote its CCTV surveillance camera network expresses the same sentiment: "[i]f you've got nothing to hide, you've got nothing to fear."[140] Similarly, Google CEO Eric Schmidt opined in a 2009 interview that "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place."[141] This worldview assumes that all those who evade, block, or protest government surveillance are hiding evidence of criminal wrongdoing.[142] Consider again the controversial stop-and-frisk policies of the NYPD. In 2011, just over half of the stops these officers conducted were justified on the observation of "furtive movement" (as opposed to, for instance, fitting a known description or carrying a suspicious object).[143] Leaked documents from the National Security Agency in 2013 revealed that the use of encryption tools alone raised red flags warranting heightened government attention.[144] The pervasiveness of this narrative,[145] widely accepted by the general public as well as the police,[146] when compounded by the extreme deference accorded to the police, means that privacy protests can be easily classified with criminal acts.

---

138. *Id.* at 39.

139. Daniel Solove in particular has critiqued this model of privacy at length in his scholarship, most recently in NOTHING TO HIDE 22 (2011).

140. *Id.* at 21–22.

141. theyTOLDyou, *Google CEO Eric Schmidt on Privacy*, YOUTUBE (Dec. 8, 2009), http://www.youtube.com/watch?v=A6e7wfDHzew&noredirect=1 (interview with CNBC).

142. As privacy expert Bruce Schneier notes, the problem with the nothing-to-hide argument is that it equates calls for privacy with "hiding a wrong." *See* Bruce Schneier, *The Eternal Value of Privacy*, WIRED (May 18, 2006), http://www.wired.com/politics/security/commentary/securitymatters/2006/05/70886.

143. *See* NYCLU report, *supra* note 126, at 4 (breaking down reasons for 2011 stop-and-frisks).

144. *See* U.S. DEP'T OF DEFENSE, EXHIBIT B § 5(3)(a) (2009), *available at* http://www.guardian.co.uk/world/interactive/2013/jun/20/exhibit-b-nsa-procedures-document (permitting "retention of all communications that are enciphered or reasonably believed to contain secret meaning" for inadvertently collected domestic communications); *see also* Andrew Leonard, *Now the Government's Cracking Down on Privacy Tools!*, SALON (June 21, 2013, 9:38 AM), http://www.salon.com/2013/06/21/how_to_get_the_nsas_attention/ (noting that "if you use encryption to make your communications private, and the NSA discovers that, it can grab your data and hold on to it until it cracks the code).

145. One Twitter user set up an account after the NSA revelations called "Nothing to Hide" that showed "tweets" from others expressing a lack of concern about government surveillance. *See* Ross Douthat, Editorial, *Your Smartphone is Watching You*, N.Y. TIMES, June 9, 2013, at SR11.

146. Justice Scalia also expressed the sentiment in California v. Hodari D., 499 U.S. 621, 623 n.1 (1991) (citing Proverbs 28:1) ("The wicked flee when no man pursueth.").

Moreover, to the extent that the police may interpret privacy protests as deliberate challenges to police authority, this may further encourage the police to investigate when no criminal wrongdoing is present. Sociologists have repeatedly demonstrated that perceived disrespect for the police is an important—indeed perhaps the primary—factor in determining the degree to which police interfere with an individual's liberty.[147] In this sense, then, the privacy protestor might present the worst sort of affront to the police: someone who appears to have something to hide and is proud of it.

These privacy protests incur costs well beyond individual embarrassment, discomfort, and wasted time. Large numbers of erroneous and seemingly unjustified police stops and arrests can reduce the public trust in the police.[148] This effect is hardly symbolic, for erosion of trust can result in greater noncompliance with the law, as well as refusals to cooperate when the police seek witnesses and volunteered information.[149]

D. How Privacy Protests Figure in Policing

Privacy protests do not affect all forms of police investigation. They have little importance in traditional investigative techniques that target a specific person or group of people based on previously gathered intelligence. When the police are investigating a known suspect regarding a homicide, for example, those who engage in privacy protests are not likely to arouse police suspicion.

Where privacy protests do matter, however, are cases where police have neither prior intelligence nor a known target. Instead, the police start out with a

---

147. The most famous among these is John Van Maanen's description of the "asshole": a person who challenges the authority of the police and thus is most likely to become the recipient of "street justice." *See* John Van Maanen, *The Asshole*, *in* POLICING: A VIEW FROM THE STREET 221, 224 (Peter K. Manning & John Van Maanen eds., 1978); *see also* Donald J. Black, *The Social Organization of Arrest*, 23 STAN. L. REV. 1087, 1108 (1971) (observing that the "probability of arrest increases when a suspect is disrespectful towards the police"); William A. Westley, *Violence and the Police*, 59 AM. J. SOC. 34, 38 tbl.1 (1953) (reporting on survey in which "disrespect for police" was the most common reason for the use of violence against individuals).

148. Taslitz, *supra* note 99, at 11; *see also* Atkinson, *supra* note 10, at 1527 (noting the costs of "empty searches" include "loss of bodily integrity, dignity costs, violation of personhood, loss of freedom, damage to reputation, and loss of privacy" (internal citations omitted)).

149. Tom Tyler has written extensively about the importance of procedural justice—that people believe the police use fair procedures—on individual legal compliance. *See generally* TOM R. TYLER, WHY PEOPLE OBEY THE LAW (2006). More specifically, Tyler has also argued that perceptions regarding the legitimacy of police authority—the feeling of obligation to obey the law—also have a significant effect on legal compliance. *See, e.g.*, Tom R. Tyler & Jeffrey Fagan, *Legitimacy and Cooperation: Why Do People Help the Police Fight Crime in Their Communities?*, 6 OHIO ST. J. CRIM. L. 231, 267 (2008) ("Cooperation increases . . . when citizens see the police as legitimate authorities who are entitled to be obeyed.").

legal violation and look for evidence and criminals.[150] The targets are unknown because the police are "trolling" or "fishing" for suspects.[151] In such instances, the police have an offense or a group of offenses they are interested in investigating, and seek patterns of suspicious activity that might identify potential suspects.

Police efforts to uncover terrorist activity exemplify these open-ended investigations. Unlike many other kinds of crimes, terrorism is an offense that places special emphasis on preventive policing. Added to these pressures is the highly secretive nature of terrorist planning. In response, police rely primarily on two options: covert policing, which requires the penetration of closed criminal groups, and the identification of patterns of suspicious activity.[152] In this latter approach, the police look for behaviors and activities that suggest the planning or execution of terrorism plots without necessarily having any particular person or activities in mind.

Privacy protests are also relevant as technologies expand surveillance capacities. This *bureaucratic surveillance* makes possible the collection of large quantities of data that can be sifted through multiple times for multiple purposes. The ubiquity of such surveillance changes the very nature of policing, as New York's Court of Appeals recently observed. Technological innovations—in that case, a GPS unit—give the police a "new technological perception of the world" that is equivalent to the addition of "millions of additional police officers" in every city.[153]

III. RECOGNIZING AND PROTECTING PRIVACY PROTESTS

The police will likely consider privacy protests as annoyances or distractions, to the extent that they attract police attention without producing evidence of criminality. Nevertheless, privacy protests can serve several socially useful purposes.

A. What Privacy Struggles Mean

First, privacy protests can raise doubts about the necessity of a particular method of governmental surveillance.[154] Some investigative techniques are highly effective, yet on balance they may be too intrusive to be practicable if they

---

150. In his study of undercover policing, Gary Marx uses a similar approach in classifying covert operations: by the specificity of target selection and prior intelligence. *See* GARY T. MARX, UNDERCOVER 70 (1988).

151. *See id.*

152. *See, e.g.*, CTR. FOR LAW AND SEC., N.Y.U., TERRORIST TRIAL REPORT CARD: SEPTEMBER 11, 2001–SEPTEMBER 11, 2011, at 3–4 (2011) (observing heavy reliance on informants and undercover operations in federal terrorism prosecutions after 9/11 terrorist attacks as part of "preventive law enforcement"); Malia Wollan & Charlie Savage, *Holder Tells a Muslim Group Sting Operations Are 'Essential*,' N.Y. TIMES, Dec. 12, 2010, at A34.

153. People v. Weaver, 909 N.E.2d 1195, 1199 (N.Y. 2009) (holding that GPS receiver placement requires a warrant).

154. *Cf.* LYON, *supra* note 1, at 164 ("If the system is accepted as legitimate and necessary, then it is unlikely that anyone will question it . . . .").

generate widespread privacy protests. In other cases, privacy protests might draw attention to the fact that certain surveillance techniques, such as facial recognition software,[155] are not particularly effective at catching criminals.

Second, actions intended to object to government surveillance can reveal beliefs about the legitimacy of public institutions. Researchers have shown that the perception of unfair treatment at the hands of the police can lead to doubts about the legitimacy of the police generally.[156] Through their actions, privacy protestors can raise questions about governmental overreaching. The more widespread the privacy protests, the more we might infer a serious lack of trust in a particular public entity.

Third, privacy protests can demonstrate the shifting boundaries of privacy norms. As surveillance capabilities increase, so too do the possibilities for intrusions into individual privacy. Many enhanced opportunities for information gathering will be met with little resistance. This is especially the case when the distribution of benefits is tied to compliance. For instance, in 2011, the Indian government began building a massive biometric database, known as Aadhaar ("foundation") that records iris and fingerprint data so that individuals can receive government benefits through nearly instant verification of their identity.[157] The acceptance of increased surveillance can also erode existing privacy norms. In some instances, however, privacy protests have the capacity to push privacy norms in the opposite direction, by forcing the abandonment of certain surveillance techniques or by producing regulatory changes.[158] By forcing the state to negotiate and compromise in some instances, privacy protests reveal that privacy norms are the product of "game-like processes."[159]

Put another way, privacy protests demonstrate an important struggle over privacy norms, even if these protests lack the coordination of a self-conscious movement. The social significance of individual resistance was famously chronicled by political scientist James Scott in his study of the inhabitants of a small Malaysian village, Sedaka, in the 1970s.[160] Scott lived with and observed the villagers of Sedaka at a time of rapid economic change and social conflict between rich Chinese landowners and Malay peasants. Scott uses his example to address the issue of why the poor do not openly revolt. The evidence suggested to Scott that the peasants were neither unaware of their situation nor passively accepting of it. Indeed, the poor of Sedaka, while choosing not to engage in open revolt against

---

155. *See* Emspak, *supra* note 67 (reporting that facial recognition software the TSA uses has yet to catch any terrorists).

156. TOM R. TYLER & YUEN J. HUO, TRUST IN THE LAW 15 (2002) (arguing that public belief in the fairness of police actions influence their acceptance of police decisionmaking).

157. *See* Lydia Polgreen, *Scanning 2.4 Billion Eyes, India Tries to Connect Poor to Growth*, N.Y. TIMES, Sept. 2, 2011, at A1.

158. *See* LYON, *supra* note 1, at 161 (referring to surveillance as a "dynamic and fluid process").

159. *Cf. id.* at 165 (using the phrase to define struggles over surveillance).

160. SCOTT, *supra* note 35, at xvii.

their perceived oppression at the hands of wealthy landowners, did in fact succeed in multiple acts of covert, private, and individual resistance.[161]

These "weapons of the weak"—character assassination, foot dragging, and petty theft, among others—constitute important forms of protest, though they are not revolutionary in any conventional sense.[162] Scott's analysis shows that the path of individual resistance against perceived oppression will take into account resource limitations as well as the likely success of more radical action. Similarly, a person engaged in a privacy protest is not only engaging in an idiosyncratic rant, but also in an act of resistance. When repeated by multiple actors, such protests have the potential to undermine the efforts of the police.[163] In some cases, these struggles hold the potential to produce regulatory change.[164]

B. Governmental Responses

A central claim in this Article is that ignoring the differences between privacy protests and efforts to hide criminal wrongdoing is a mistake, for privacy protests can hold social value. If that is the case, as the previous sections have argued, how should government respond?

At the outset, it should be clear that the elimination of governmental surveillance is not only impracticable but undesirable. Modern states need surveillance to govern.[165] If they are to distribute goods, understand the needs of their citizens, and provide security, governments must collect some amount of information from individuals.

At the same time, the refusal to recognize privacy protests, particularly if they are numerous enough, can pose potentially significant challenges for efficient governance. From a practical standpoint, the government can likely tolerate some number of privacy protests and still pursue its goals of collecting information and identifying noncompliance and wrongdoing. When a sufficient number of people refuse to cooperate, however, they pose a threat to the ability of government to exist, because the government is dependent on individuals submitting to inspection, presenting their identification, and behaving in apparently law-abiding ways.[166]

Faced with a sufficient enough number of privacy protests, the government might meet resistance with greater coercive force on its own part to collect information. Or, the government might provide incentives to individuals to

---

161. *Id*. at 241–303.

162. *Id*. at 29.

163. *Cf. id*. at 35–36 ("Multiplied many thousandfold, such petty acts of resistance by peasants may in the end make an utter shambles of the policies dreamed up by their would be superiors . . . .").

164. LYON, *supra* note 1 at 161.

165. *See* Garland, *supra* note 8, at 3; *cf.* LYON, *supra* note 1, at 177 (observing that surveillance is an "unavoidable aspect of living in twenty-first century societies").

166. *See* LYON, *supra* note 1, at 164 ("If people did hesitate [in providing requested information], let alone withdraw willing cooperation, everyday social life as we know it today would break down.").

encourage greater voluntary compliance.[167] The government might also engage in responsive strategies to thwart those who are themselves trying to thwart state surveillance.[168]

These responses attempt to eliminate rather than understand privacy protests, however. If privacy protests represent legitimate struggles with the state over privacy norms, then a government committed to a robust definition of privacy should incorporate some of those views.

1. Legislative Responses

Privacy protests can play a role in prompting legislatures to consider whether they have paid sufficient interest to privacy concerns when law enforcement agencies adopt new surveillance technologies. The introduction of domestic drones is a good example. The 2012 Federal Aviation Administration ("FAA") reauthorization law ordered the agency to create a regulatory framework for public safety agencies to fly unmanned drones in American airspace by 2015.[169] By the FAA's own estimates, some 30,000 drones operated by the government, as well as by private entities, could be in American airspace by 2020.[170] In its initial response to privacy concerns raised by civil liberties groups and by some members of Congress, the FAA acknowledged that the use of unmanned drones within the United States presented "privacy concerns" while at the same time emphasizing its primary mission of ensuring the safety and efficiency of the National Airspace System.[171] In response, some members of Congress have proposed legislative protections. Representative Edward Markey introduced the proposed Drone Aircraft Privacy and Transparency Act in December 2012, which would require specific privacy protections in drone use, such as presumed warrants for the police, disclosure requirements, and data

---

167. Scott makes both of these points as potential state reactions. *See* SCOTT, *supra* note 35, at 36.

168. *See* Gary Marx, *A Tack in the Shoe and Taking Off the Shoe: Neutralization and Counter-neutralization Dynamics*, 6 SURVEILLANCE & SOC'Y 294, 294 (2009). Marx refers to such responses as counter-neutralization techniques. *Id.*

169. FAA Modernization and Reform Act of 2012, Pub. L. No. 112–95, 126 Stat. 11 § 332; *see also FAS Makes Progress with UAS Integration*, FAA.GOV (May 14, 2012), http://www.faa.gov/news/updates/?newsId=68004; Andrea Stone, *Drone Program Aims to 'Accelerate' Use of Unmanned Aircraft by Police*, HUFFINGTON POST (May 22, 2012, 5:30 PM), http://www.huffingtonpost.com/2012/05/22/drones-dhs-program-unmanned-aircraft-police_n_1537074.html.

170. *See, e.g.*, S. Smithson, *Drones over U.S. Get OK by Congress,* WASH. TIMES (Feb. 7, 2012), http://www.washingtontimes.com/news/2012/feb/7/coming-to-a-sky-near-you/?page=all.

171. Letter from Michael P. Huerta, Acting Admin. of the FAA, to Representative Edward J. Markey (Sept. 21, 2012) (on file with Author). The FAA also announced, without further specification, that it would incorporate "privacy concerns" into the planning of six test sites for unmanned drones mandated by Congress. *See id.*

collection minimization.[172] State and local governments are also debating what privacy protections might be required for police-operated drones.[173]

These privacy protections may not necessarily become law. And even if some privacy legislation is enacted, it may impose relatively weak controls on drone use by the police. In this scenario, one can easily imagine protests by grassroots and civil liberties organizations. Another relevant consideration may be the existence of privacy protestors: individuals unaffiliated with any particular group who engage in acts of resistance. This might involve changing personal habits or altering one's home to block aerial surveillance. Designer Adam Harvey, for example, has designed "anti-drone" wear inspired by burqas and made of metallized fabric designed to thwart thermal imaging surveillance.[174]

2. Judicial Responses

Not all privacy protests target new expansions of governmental surveillance capabilities. Many privacy protests—the closed blind or the aversive walk—are low-tech objections to "ordinary" police surveillance. As discussed earlier,[175] because the Supreme Court has not heavily regulated the police in their exercise of discretion, police judgments about suspicious behavior can easily—and erroneously—target noncriminal privacy protests.

Instead of granting extreme deference, courts should require police to be more exacting in their judgments about suspicious behavior so that privacy protests are less likely to be mistakenly targeted.[176] In theory, both search warrant applications and suppression hearings provide judges with the opportunity to evaluate police assessments of suspicion.[177] Prosecutors also provide an independent level of review when they assess cases for prosecution.[178] Yet in practice, few applications are denied,[179] and successful motions to suppress are the

---

172. Drone Aircraft Privacy and Transparency Act of 2012, H.R. 6676, 112th Cong. §§ 339(c), 340, 341(a) (2012).

173. *See, e.g.*, Somini Sengupta, *Rise of Drones in U.S. Drives Efforts to Limit Police Use*, N.Y. TIMES, Feb. 16, 2013, at A1.

174. *See* Adam Harvey, *Stealth Wear*, AHPROJECTS.COM, http://ahprojects.com/projects/stealth-wear (last visited Oct. 6, 2013).

175. *See supra* Part III.B.

176. *See* Taslitz, *supra* note 99, at 32 ("The more robust the individualized suspicion requirement, and the more it incorporates the insights of modern cognitive science, the greater the impetus for appropriate training, wherever feasible.").

177. *See id.* at 64.

178. *See* Marc L. Miller & Ronald F. Wright, *The Black Box*, 94 IOWA L. REV. 125, 137–41 (2008).

179. *See, e.g.*, RICHARD VAN DUIZEND ET AL., NAT'L CTR. FOR STATE COURTS, THE SEARCH WARRANT PROCESS: PRECONCEPTIONS, PERCEPTIONS, AND PRACTICES 32 (1985) (finding that in a study of seven cities that magistrates "rarely deny an application for a search warrant").

exception rather than the rule.[180] Many commentators attribute this deference to judicial attitudes that highly credit police intuition.[181]

Courts should enforce a more rigorous individualized suspicion requirement. When courts require more of the police, officers have greater incentives to engage in more thorough investigations.[182] A more rigorous approach to Fourth Amendment suspicion might impose upon the police a duty to investigate their initial intuitions and assumptions in some cases.[183] In many cases, a police officer can and should investigate further to confirm or dispel an initial hunch.[184]

Finally, courts should acknowledge that attempts to evade police surveillance may be as indicative of privacy protection as it is of criminal guilt. An encrypted file may hide contraband, but it can just as easily protect legitimate privacy concerns.[185]

3. Police Training

Police departments can also do more to draw attention to the differences between privacy protests and truly suspicious activity indicative of crime. Police training can clarify that suspicious activity may be truly innocent activity that requires further investigation and confirmation. Even if the Fourth Amendment does not curb police discretion in significant ways, departments can encourage investigative techniques that call for informed decisionmaking. Departments should encourage officers to verify hunches to rule out innocent explanations.[186]

---

180. The available studies suggest that only a small minority of motions are ever granted. *See, e.g.*, U.S. COMPTROLLER GEN., GGD-79-45, IMPACT OF THE EXCLUSIONARY RULE ON FEDERAL CRIMINAL PROSECUTIONS 11 (1979) (suppression motions granted in 1.3% of 2,804 federal cases); VAN DUIZEND ET AL., *supra* note 179, at 26 (motions to suppress are granted in 5% of prosecutions); Peter F. Nardulli, *The Societal Cost of the Exclusionary Rule: An Empirical Assessment*, 1983 AM. B. FOUND. RES. J. 585, 598 tbl.8 (successful motions to suppress physical evidence occurred in 0.69% of 7,484 cases sampled).

181. *See, e.g.*, Harris, *supra* note 120, at 999.

182. That the exclusionary rule serves as a deterrent to the police is a subject of much debate, but at the very least, there is likely *some* deterrent effect from its existence. *See, e.g.*, Taslitz, *supra* note 99, at 65 (noting at least "some modest deterrent effect").

183. *See id.* at 57 (explaining that a "speculate and test" model can be incorporated into the probable cause determination by requiring a duty to investigate).

184. *See id.*

185. In this respect, the Ninth Circuit's decision in *Cotterman* reflects the "nothing to hide" assumption: File encryption, without more, may support a finding of reasonable suspicion. *See* United States v. Cotterman, 709 F.3d 952, 969 (9th Cir. 2013) (permitting use of password-protected file as part of reasonable basis analysis). Notably, the *Cotterman* majority did not think that encryption of an entire computer necessarily constitutes a relevant factor. *Id.* at 969 n.17.

186. *See* Taslitz, *supra* note 99, at 57.

Departments should also provide officers with data about the relative successes and failures of specific strategies, such as the use of profiles.[187]

This attention to potentially innocent activity is particularly important in mass surveillance programs that collect large amounts of data to be sorted according to discretionary criteria. While the simple collection of this information may be value neutral, what is tagged as suspicious depends on subjective definitions of unusual behavior. The federal government's Suspicious Activity Reporting ("SAR") initiative, which encourages local police departments to identify and record suspicious activity that can be shared on a nationwide computer network, relies on discretionary criteria to sort innocent from suspicious activity.[188] To the extent that any suspicious activity is consistent with privacy protests, police departments should minimize or avoid the targeting of potentially innocent behavior.[189]

In a more traditional policing context, departments can influence individual officer behavior by changing incentives.[190] Many factors drive the decisions of individual patrol officers, but chief among them are departmental cultures that emphasize high numbers of stops or arrests—whether by promoting a culture of aggressive policing or even by operating informal quotas.[191] A

---

187. *See id.* at 58; *see also* David H. Bayley & Egon Bittner, *Learning the Skills of Policing*, 47 LAW & CONTEMP. PROBS. 35, 50 (1984) ("What officers need . . . is information that shows what the likely results will be from the use of tactics of different sorts in various situations.").

188. *See, e.g.*, NAT'L CRIMINAL INTELLIGENCE RES. CTR., NATIONWIDE SAR INITIATIVE (2012), *available at* http://nsi.ncirc.gov/documents/Nationwide_SAR_Initiative_Overview_2012.pdf.

189. For a critical review of SAR criteria, see ACLU, *More About Suspicious Activity Reporting*, ACLU.ORG (Jan. 18, 2013), http://www.aclu.org/spy-files/more-about-suspicious-activity-reporting (observing that "the proliferation of SAR reporting programs with [low] collection standards have too often led to inappropriate law enforcement contact with completely innocent Americans").

190. *See* Taslitz, *supra* note 99, at 60 (noting that incentives are important to the decisionmaking environment).

191. While few departments would admit to formal quotas regarding arrests, stops, or tickets, stories abound regarding informal or secret directives directed to rank-and-file officers. *See, e.g.*, Al Baker & Ray Rivera, *On Secret Tape, Police Press a Tickets Quota*, N.Y. TIMES, Sept. 10, 2010, at A1 (reporting on secret audio tape that recorded an NYPD police captain as requiring twenty summonses a week); David Burnham, *Performance Level Set in a Police Test*, N.Y. TIMES, Mar. 9, 1973, at A1 (describing discovery of "Operation Prod," in which police officers in 15 Brooklyn precincts would be punished for failing to make arrest and ticket quotas); Justin Jouvenal, *Fairfax County Police Ticket Policy Scrutinized*, WASH. POST. (Jan. 20, 2013), http://articles.washingtonpost.com/2013-01-20/local/36473708_1_ticket-quotas-police-supervisors-officers (describing summons quota discovered for Fairfax county police). In 2010, former NYPD Officer Adrian Schoolcraft filed a lawsuit against the department in which he claimed retaliation for reporting manipulation of crime statistics and the use of ticket and arrest quotas. *See* Al Baker & Ray Rivera, *5 Officers Face Charges in Fudging of Statistics*, N.Y. TIMES, Oct. 16, 2010, at A13; *cf.* Rhonda Cook, *Ex-Officers: APD Had Arrest Quotas*, ATLANTA J. CONST. (Jan. 14, 2013), http://www.ajc.com/news/news/crime-

generation ago, sociologist Jerome Skolnick observed that the "'constant' pressure to appear efficient" explains why patrol officers feel compelled to produce arrests and tickets.[192] These pressures further encourage the types of cognitive shortcuts that fail to distinguish criminal behavior from the odd, the nonconforming, and the privacy protest.[193]

CONCLUSION

Privacy protests often appear no different from criminal evasiveness, but they merit recognition as important sources of resistance to the increasing capabilities of government surveillance. These individual, ad hoc, and spontaneous attempts to thwart police surveillance are as worthy of attention as organized protests, public interest litigation, and media criticism with the same objectives. Yet privacy protests have largely escaped legal attention, in large part because Fourth Amendment law makes little distinction between the ordinary criminal's evasions and the privacy protest. The absence of a distinction raises the risk that the police will unnecessarily target privacy protestors and blinds us to their potential social value. Although not every privacy protest will enhance our understanding of privacy, many will. That understanding cannot take place until we recognize these acts of resistance.

---

law/ex-officers-apd-had-arrest-quotas/nTwtX/ (reporting on lawsuit in which former Atlanta police officers filed affidavits conceding they were acting according to quotas).

192. SKOLNICK, *supra* note 97, at 44.

193. *Cf.* United States v. Brignoni-Ponce, 422 U.S. 873, 889 (1975) (Douglas, J., concurring) (noting that the "nature of the [*Terry v. Ohio*] test permits the police to interfere as well with a multitude of law-abiding citizens, whose only transgression may be a nonconformist appearance or attitude").