This is the copyedited final text; however, pagination differs slightly from the print. Please cite as Stalcup, M (2015) Policing Uncertainty: On Suspicious Activity Reporting. In: Saminian-Darash, L and Rabinow, P (eds) *Modes of Uncertainty: Anthropological Cases*. Chicago: Chicago University Press, 69-87.

CHAPTER FOUR

Policing Uncertainty
On Suspicious Activity Reporting

MEG STALCUP

Introduction

Several of the men who would become the 9/11 hijackers were stopped for minor traffic violations.[1] Mohamed Atta was cited for driving without a license in Florida near the end of April 2001. When he failed to appear in court, a warrant was issued for his arrest. The warrant, however, seems not to have been flagged properly, since nothing happened when Atta was pulled over again, for speeding.

In the government inquiries that followed the events of 11 September 2001, and in the press, these brushes with the law were missed opportunities. But for many police officers in the United States,[2] they were moments of professional revelation and were also personally fraught. "It is always a local cop who saw something," said the deputy director of an intelligence fusion center.[3] He replayed for me how the incidents of contact had unfolded with the men and the uncertainty of every encounter, whether a traffic stop or someone taking photos of a landmark.

Shortly after 9/11, major professional organizations for US law enforcement mobilized a series of working groups. Funded by the Department of Justice, these brought together leading city- and state-level law enforcement from around the country, and representatives from federal agencies. The groups worked on designing policies to include police officers in national intelligence,[4] producing detailed recommendations and plans. Among these was what would eventually come to be the Suspicious Activity Reporting Initiative. Through its operation, police officers, as well as members of the public and industry, could submit tips and incidents of note from the ground. In turn, the federal government would communicate to participants timely information on security threats. While state, local, tribal, and federal governments; citizens; and those in the

private sector were all included in the initiative, the network was organized around fusion centers and the work of police, who centrally designed both.

The idea was to capitalize on what patrol officers already did when dealing with the general public. An officer who sees someone behaving suspiciously will observe and decide whether or not to write up the incident. This routine documentation of suspicious activity was systematized into steps for gathering, evaluating, and sharing information. An incident report is sent from the police department to dedicated intelligence specialists for evaluation. They may decide that an incident was innocuous or ordinary crime, in which case the submission is referred back to the local police or to an apposite task force. However, if an incident seems, in official language, to also be "reasonably indicative of preoperational planning related to terrorism or other criminal activity" (US DOJ 2010:1) a Suspicious Activity Report (SAR) is created and uploaded through portals to the shared network spaces of a number of government agencies, and fusion centers participating in the Initiative. An FBI team of local officers and federal agents from various departments called a Joint Terrorism Task Force may be part of the decision process or notified subsequently, in order to take operational action if warranted.[5]

The design of the initiative was distinctively anticipatory. Suspicious behaviors were taken as the precursors of a threat that was still in virtual form. Officers and intelligence analysts already cultivate a relationship to uncertainty as part of their expertise, and their very subjectivity. The problem they faced in this undertaking was not how to collect ever more information (others were engaged in that task). Nor was it how to associate disparate pieces of a plot in order to predict or preempt the future (this is a later step). Instead, their task was to detect a potential event, by discerning elements of the pre-event (Samimian-Darash 2009). The uncertainty inherent in the public activities they watched and analyzed had to be parsed, but without over determining a situation with potential that, as the traffic stops of the hijackers had shown, could exceed known or speculated possibilities.

Events can be prevented, preempted, and anticipated, among other approaches, and in this chapter I look at these three as technologies of security in US counterterrorism, focusing on their differing modes of uncertainty. Prevention arises from the roots of risk (Ewald 2002), where uncertainty is a function of lack of knowledge. The same knowledge used to define a risk also supports efforts to address causes, to stop the threat from manifesting. Yet prevention has temporal limits (it cannot address an imminent threat), as well as epistemological ones (uncertainty comes not only from what one does not know, but from the potential inherent in the virtual for something else to

happen). Preemption deals with the virtual by instigating the manifestation of threats to better manage the actual form taken (Massumi 2007). To these two technologies, already well-described in the literature,[6] I add anticipation. Through empirical analysis of the Suspicious Activity Reporting Initiative, I suggest anticipation deals with potential uncertainty; not by creating possibilities, but by detecting precursor events as they actualize. The initiative relies on the capacity of officers and analysts to discern suspicion, which entails a distinct mode of uncertainty, particularly in the subjectivation of police officers and intelligence analysts. Finally, I place "policing uncertainty" within a broader national intelligence counterterrorism assemblage and the governance of security.

Technologies of Security: Preemption, Prevention, and Anticipation

Experts of war traditionally separated preemption and prevention in relation to uncertainty, which had a significant temporal dimension (Macedo 2008).[7] A threat could be both certain and imminent, as when an invasion was mobilized and on the border of a country. Under such circumstances, preemption was understood as akin to throwing the first punch against an already circling opponent (Doyle 2008, 81). Preemption in this sense had a narrow window, and moreover was necessarily unusual, because complex real-world scenarios rarely offer certainty, and determined attackers (those very ones about whom one is likely to be certain) do not want to publicize their imminent action. When the threat of the enemy was admittedly possible, yet uncertain or at some remove in time, then one was understood to act "preventatively," in what was viewed as an act of aggression. Prevention could be a desire "to fight sooner rather than later" (Mueller et al. 2006, 9), or to keep enemies from acquiring "threatening capabilities" (Doyle 2008, 20), such as nuclear weapons. But with the threat neither certain nor imminent, prevention as an act of war was not justified under dominant traditions of international law.

Preemption

Following the events of 9/11, the Bush administration *relabeled* prevention as preemption.[8] In the Bush Doctrine, a preemptive blow was one taken first, but unlike in previous war doctrine, the condition of certain, imminent threat was removed. One attacked sooner, rather than later. The justification for this shift in the meaning of preemption was an ontological change in the nature of threat. "At the perilous crossroads

of radicalism and technology," President George W. Bush said in a June 2002 speech, "even weak states and small groups could attain a catastrophic power to strike great nations." Therefore, he added, "if we wait for threats to fully materialize we will have waited too long" (Bush 2002). Waiting for certainty, which is to say, waiting to be sure of the threat, could have potentially catastrophic consequences; both certainty and the period of inaction were therefore refused. Preemption now not only did not require certainty, it *required* uncertainty. It was precisely because of what *could* happen (if preemptive action wasn't taken), linked to the potential for devastating consequences, that acting was justified sooner rather than later.[9]

What the re-defined Bush Doctrine of preemption tackled was the problem of virtuality. The United States' preemptive attack on Iraq in 2003 was launched because Saddam Hussein might have had weapons of mass destruction, and the potential (both for the weapons' existence and their destructive capacity) provided the grounds for action (Massumi 2007). Although the weapons were not found, in claiming potential uncertainty as the grounds for taking action, the decision to act could not be wrong. Hussein always "*could have* restarted his weapons projects at any moment" (ibid.). With a virtual cause, no single actualization can exhaust potential.

Preemption addresses the problem that the virtual poses for security by precipitating its actualization, making potential take "a shape to which it hopes it can respond" (Massumi 2007). Guided by a desire not to limit action to plan for what may be the incorrect future, potential uncertainty is brought directly into the sphere of governance. Louise Amoore and Marieke de Goede describe, for example, how transactions data, such as personal remittances sent abroad or the purchase of fertilizer, are quietly collected, archived, and used "to identify a suspicious body in movement and, most importantly, to verify or deny access *in advance*" (2008, 173). As with the Bush Doctrine's preemptive war, action—stopping someone from boarding an airplane for example—is not taken on the basis of knowledge, the mass of collected data about the person, but on "an absence, on what is not known, on the very basis of uncertainty" (Amoore 2011, 27). The potential for threat in this uncertainty leads to preemptively denying entrance or access. Although the algorithms do not produce causal patterns, and they do continuously adapt by incorporating their own results and new data, they are nonetheless "an already encoded set of possibilities" (Amoore 2011, 34). Potential is preemptively turned into possible futures that emerge from the knowledge, imagination, and judgment of the software developers who create and refine the algorithms. These are assigned to travelers as they catch trains or wait at borders: losses of liberty, sometimes

small, sometimes great, that constitute the "banal face of the preemptive strike" of the war on terror (Amoore and de Goede 2008, 173).

Prevention

Next in the trio of governmental technologies discussed here, "prevention" traces genealogically from a nineteenth-century approach to insecurity (rather than war doctrine's concern with what counts as just war) that was "tied to a scientific utopia ever more capable of controlling risks" (Ewald 2002, 282). Risks in this specific sense are those threats for which probability can be calculated from knowledge about the past. François Ewald noted that the identification of risk presupposes "science, technical control, the idea of possible understanding, and objective measurement." One way of dealing with risk is insurance, which shares risk among a broader social body and compensates individuals for harm suffered. The same knowledge that grounds insurance, with its calculation of damage and compensation, also provides the basis for prevention. Instead of compensating for someone's losses, expertise in prevention seeks to reduce "the probability of their occurrence" (ibid.); the effort is focused on root causes, so that a threat is not realized.

Preventative practices assume that a targetable threat exists prior to intervention (Massumi 2007). The preventative approach to "homegrown terrorism" in the United States, for example, takes such acts to result from "radicalization to violence" inspired but not directed by a foreign terrorist organization. The terms and terrain of action pertain to arenas of expertise that have defined the threat: specialists in radicalization. In the Executive Office of the President's official Countering Violent Extremism strategy (2011) homegrown terrorism is indexed to and dealt with by "mental health experts, juvenile justice officials, and law enforcement" (4), especially those with counter-gang experience. Ewald explicates (2002, 297): "The logics of fault and prevention presuppose that, in the spheres they govern, it is always possible to articulate a standard of conduct that everyone must observe." For the purposes of CVE strategy, the causes of radicalization are divided into categories: poor mental health, lack of opportunity, social pressures. The strategy targets sets of behaviors through which radicalization could be sparked and fed, such as associating in person or online with other extremists, reading extremist literature, and making speech acts.[10]

Ewald describes prevention as "a rational approach to an evil that science can objectify and measure" (2002, 293). Such techniques create the need for more and more

information. With enough of the right information, this approach assumes, violent extremists can be assessed empirically to identify what caused their radicalization. The "predictable, linear course from cause to effect" (Massumi 2007, 5) that these preventative efforts posit does not need, nor account for, potential uncertainty.[11]

Anticipation

Prevention and preemption, although but two approaches to security, are a useful dyad to triangulate with anticipation in order to distinguish it as a distinct approach.[12] Prevention centers around causes that hold a direct relationship to possible and knowable effects. In a preventative mode, uncertainty is the result of having insufficient information, and can be addressed by collecting data, calculating probabilities, or identifying at-risk populations. Preemption instead confronts a virtual threat by creating possible futures and bringing them into existence. A preemptive mode is one in which future potential uncertainty is made real in the present.

Anticipation also deals with potential uncertainty, but instead of instigating or delimiting events, configures a time and space of waiting, poised and vigilant, to detect the moments that precursor incidents appear. This targets an intermediary stage of event emergence, in which prevention has been unsuccessful but the threat has not yet taken a definitive form. In this "in between," the anticipatory technology amplifies inconspicuous components of the interval in which an event is coming into existence, its becoming period. Like other "event technologies" (Samimian-Darash 2013), this means that anticipation does not deal with future potential by predicting the future. Instead, anticipation aims to make the pre-event itself governable.

One meaning of anticipation is to predict what will happen and to take action in order to be prepared; exercises, scenarios, and other imaginative methods of taking up the future present abound in government practice. "To anticipate," however, is also to act as a forerunner or precursor, and this is how suspicious activities are understood to anticipate the event. The SAR technology seeks to capture minor incidents that could build into a major attack; it attends to not the threat itself but its precursors. These building blocks could be assembled into any number of final shapes in the future, but even without clairvoyance they can also be knocked out of place if identified, or serve as clues to underlying plans.

If one considers the full "time of the event," the past and future which inhere in

time and divide each present infinitely (Deleuze 1990, 5), the incidents occur in the becoming period. When instances of the would-be terrorist's "preoperational planning" are identified as suspicious activities, there has not yet been a terrorist event, and the intent is that it is never to be. Anticipatory technology configures this pre-event period rather than the event itself, because a virtual event could always exceed the knowable possibilities or prepared-for contingencies. However, while incidents that police officers observe may be forerunners to terrorist events, the event itself remains undetermined by and external to the anticipatory technology.

Michel Foucault suggested that disciplines crossed a kind of "'technological' threshold" when "they attained a level at which the formation of knowledge and the increase of power regularly reinforce one another in a circular process" (1977, 224). Building on Foucault's conceptualization, Mitchell Dean (1996) argued that "practices of government" could attain a technological orientation: "when their assemblage evinces a certain kind of strategic rationality. The general form of this strategic rationality is one that brings governmental requirements of conduct into a kind of perpetual loop with technical requirements of performance" (61). Officers and analysts are constituted as "subjects of performance" in enacting the technology (ibid.). If preemptive detection via algorithms relies on decisions about uncertainty made in the design or application of the formulas, suspicious activity reporting counts on subjects of performance working in a mode of uncertainty. Marking the significance of suspicious behaviors requires cultivating discernment, a capacity understood to develop through experience and training. The following sections examine how older police knowledge was adapted into a post-9/11 technology of anticipation, and the subjectivational demands made by these shifts.

Assembling an Anticipatory Technology

Suspicious activity reporting developed at least in part because loci of experience and invention outside of federal government bureaucracies were mobilized. The initiative came out of not only the usual suspects among defense contractors, the FBI, and others in the intelligence community,[13] but a "sub-state" array of venues that shape, govern, and manage daily social life– state and local government, police and legal professional organizations, civil rights and liberties activist groups, and religious advocacy organizations. The deputy director at an intelligence fusion center named what was, for him, the most significant factor: "Basically—and this was a big part—the state did not

trust the federal government. They felt that there was such a lapse that created September 11th that we needed to do our own project and track down these terrorists." The history of the formative role of sub-state organizations is passed over on federal government websites,[14] which emphasize the authorizing legal instruments from Congress and Executive Orders.[15] In fact the top-level pronouncements generally specified *what* should happen—e.g., state and local law enforcement should be included in national intelligence efforts—but offered little or nothing in terms of specifying *how*. The backstory of the two most important initiatives for the development of suspicious activity reporting, the Nationwide SAR Initiative and the National Network of State and Major Urban Area Fusion Centers, points, however, to the many effects of this shift away from federal venues and subjects.

One month after September 11th, 2001, the International Association of Chiefs of Police (IACP) announced that an "intelligence sharing summit" would be held in the spring. Recommendations from that summit proposed the core elements of what would become fusion centers (IACP 2002, iv) and suspicious activity reporting (then subsumed under "intelligence-led policing"), as well as the formation of a Global Justice Information Sharing Initiative Intelligence Working Group. A fusion center director who participated in the working group, a thirty-year career police officer before he entered management, recounted their thinking:

> There are a lot of cops in America. County and municipal and state and private cops, 850-870, 000 of them . . . post-9/11, we decided, if we train state and local cops to understand pre-terrorism indicators, if we train them to be more curious, and to question more what they see, and got them into a system where they could actually get that information to somebody where it matters . . . [we would] get cops to understand how important their role is, how they are really the first line of defense, the eyes and ears on the ground.

The working group issued the first *National Criminal Intelligence Sharing Plan* in 2003. A revised 2005 plan described an initiative by the Regional Information Sharing System centers (of which there are six), with the Department of Homeland Security, for liaising with local and state law enforcement agencies within the jurisdictional areas surrounding critical infrastructure facilities in order to support "reporting of suspicious activities and incidents." That same year, a report was issued titled *Intelligence-led Policing: The New Intelligence Architecture*. Also developed by police chiefs, management, officers, and

other public safety officials acting as representatives of police professional associations[16] and funded by the Bureau of Justice Assistance at the Department of Justice, the report mentioned fusion centers by name, and reiterated the core of idea of reporting suspicious behaviors (Peterson 2005, 11):

> Patrol officers are the eyes and ears of the police effort, and they must be encouraged and trained to look and listen intelligently. Information from field interviews, interactions with business people, and other activities and observations must be captured and forwarded to intelligence staff members who can analyze the data, arrive at appropriate courses of action, and send information back to the beat officers.

Intelligence fusion centers are physical locations for receiving, analyzing and sharing the kind of "threat-related information" that is produced by police officers reporting suspicious behaviors. Early centers grew out of existing criminal intelligence and analysis units, a pathway observed and advocated as early as the 2002 summit (IACP 2002, iii):

> A variety of law enforcement and protective services organizations already engage in substantial intelligence sharing. Rather than replicating such efforts, the [proposed] Council should seek to connect them, strengthen them, support their expansion as necessary and then fill other gaps in the current system.

By the time of 2005 publication of the *Criminal Intelligence Sharing Plan* and the *Intelligence-Led Policing* report, twenty-five fusion centers had been established, and with the 2007 *National Strategy for Information Sharing*, the federal government was politically and logistically on-board.

Counterdrug expertise would have a formative influence on the ways that law enforcement took up its new counterterrorism tasks. Before terrorism captured lawmakers' attention, counternarcotics had been funding favorites, with grants that supported the establishment of criminal intelligence and "High Intensity Drug Trafficking Area" (HIDTA) programs. HIDTAs therefore were positioned to offer infrastructural support, and to serve as one of the models for conceptualizing fusion centers. At the same time, the increased importance given to terrorism meant that formerly untouchable "war on drugs" funding was at risk, and co-location offered a way to sustain the older drug programs. The counternarcotics approach to criminal intelligence in particular, its techniques, strategies, and institutional memory, would come to be influential.

Management and analysts were drawn from the ranks of former narcotics officers, among other law enforcement subgroups. They were officers who knew how to get wiretaps on mobile phones, run informants, identify gang leaders, and map gang followers. They had experience "following the money," and spotting money laundering. All of this was viewed as applicable to counterterrorism.

Fusion center staff also came out of the military, which, engaged in simultaneous wars in Iraq and Afghanistan, was producing a pool of veteran intelligence analysts. Those who were active in the national guard had the added advantage, from the point of view of data fusion and intelligence sharing, of providing a conduit between the military and state and local governments. Defense contractors both advised and competed to provide data management and analysis tools to the new centers. As these came to be recognized and approved by the federal government, the Homeland Security Grant Funding Program was initiated,[17] and institutionalization intensified. By the time of a (highly critical) 2012 Senate review, an estimated $289 million to $1.4 billion had been spent to found some seventy centers.

Suspicious Incidents

The police officer documents the suspicious behavior of an individual, staking a claim to an element of significance in otherwise undifferentiated uncertainty. In the words of a sheriff's deputy: "Anytime you meet someone out in the field and you think you might run into them again, you would write up an FI card—a Field Incident or Field Encounter card." The impetus for such interactions is something that the person does to call attention to him or herself. This "behavioral" profiling was developed in order to avoid racial or ethnic or religious profiling (all of which are illegal). Both for the operation of anticipation and social justice, such biases raise concerns (see also Amoore and de Goede 2008). However, whether it is feasible to perceive only behavior and context or if officers really attempt to engage in strictly behavioral profiling is less the point here than the presuppositions of the process itself. The officers' capacity for discernment—marking a distinction between the ordinary and the suspicious—is assumed to allow them to detect incidents in the course of duty, in public settings, during traffic stops, or on service calls.

"Creating an incident [card] would be the next level, and a report after that," explained the deputy. "An FI card would state that you had contact with so-and-so, when and how, if cooperative or not. If you're being written up on an FI card, you are already

suspect." No causal pattern is applied, however, or future possibility projected, beyond what is required to make sense of the immediate behavior. The deputy brought up the situation of an old man down in a gully with a young boy. It could be a grandfather with grandson, but "if anything's a little odd, I document it. If the kid makes a complaint three years from now, you now have enough for a case." The details are registered because of their potential. By discerning and documenting them, instead of delimiting the future, potential uncertainty increases, as do unknowable futures.

In another example, the deputy recounted how he engaged a parolee who failed to identify himself as such. Recognizing him, and knowing that he was on parole but not the specifics of his case, the deputy said, "I want to check what his prior was for. It's more of a moral judgment." His assessment already includes an aspect of this "moral judgment;" the knowledge that the man has previously been incarcerated makes his failure to identify himself suspect. The Field Incident card, in its confined capture of the time, date, location and mechanics of the encounter, is documentation of this suspicion.

Front-line officers were meant for exactly such work, said one trainer in Florida, a former criminal investigator. The intellectual history of discernment itself is largely one of how to recognize the "signs of the times."[18] This was coupled with the question of who one had to be in order to discern such signs. Despite the shift in scale, and to the secular, these questions remained central for the trainer, and to the Suspicious Activity Reporting Initiative. The discerning officer was someone who could recognize signs by drawing on intuition that was less instinct than an experiential knowledge internalized under the intensity of adverse conditions. The internalization occurred partially in training but mostly on the job. "When you are fighting sleep, walking up and down the back alleys," said the trainer, "you come to know what does and doesn't belong. Certain things belong, certain things don't. You can tell if a car is parked in the wrong location."

Police, he said, "just need to be encouraged to do their normal jobs but maybe with better tools: better indicators, items to be on the lookout for." He had doubts about cops making the connection to terrorism. "The thing about checking a box about terrorism is, is the officer on the street going to know it is about terrorism? Or is it just a peculiar thing?" But for him, this incapacity was a strength. The officers would discern the pre-event indications of terrorism without imagining them. Their task was to engage their capacity to differentiate the ordinary from the suspicious.

Functional Standards for coding suspicious behaviors were nonetheless developed to aid officers (ISE 2008; ISE 2009). Issued in 2008 and then revised in 2009, these

provided a list of behaviors, criminal and noncriminal. Some agencies had officers apply the codes themselves, while in other places codes might be added to the officers' reports later, by a specialized unit, or at a fusion center. Behaviors defined as criminal and with potential nexus to terrorism were straightforward and uncontroversial; these included attempted intrusion and damaging or threatening to damage infrastructure. Those behaviors on the "Potential Criminal or Noncriminal Activity" list, however, fell on much less solid ground. One example was: "demonstrating unusual interest in facilities, buildings, or infrastructure beyond mere casual or professional (e.g., engineers) interest such that a reasonable person would consider the activity suspicious." Observation through binoculars, taking notes, and attempting to measure distances were listed as possible suspicious activities of this sort.

The officer would need to intuit something was wrong and articulate what it was in relation to the circumstances. An action could not be suspicious outside of context. And the officers were not supposed to *look for* those behaviors. Rather if a behavior were observed as suspicious, the codes would be used to label them. A former police officer said,

> You may have an officer who says someone is taking a photo of a bridge, and asks, "what is this person doing?" then digs a little and finds it is probably a tourist. A person is taking lots of pictures of a bridge—it may be explainable. The idea of an SAR is taking behaviors that are outside the norm, and being able to share that.

Officers have repeatedly stopped photographers, however, at times leading to the erasure of what are protected images, other times leading to arrest (Simon 2012). The nuanced shift from discerning suspicion to that which is suspicious of terrorism was harder to put into practice than it seemed in theory.

Institutionalization

From October 2008 through the end of September 2009, twelve major urban and state fusion centers participated in a test run of the initiative, called the Evaluation Environment. Each site developed a set of protocols that integrated local procedures for reporting suspicious incidents into the system that had been developed in order to share information with each other and with different entities in the federal government. At the end of the Evaluation Environment period, the final report presented a summary from

each of the twelve sites on human workflow, implementation and harmonization with existing technical systems, what training and outreach to the public had taken place, and recommendations.

The diversity of local approaches to handling information was one of the challenges of the initiative and its efforts to produce pre-event indicators. The working groups that had begun meeting in 2002 guided the intelligence processes that most major state and city departments put in place after 9/11, many of which had representatives in the groups. Local procedures were developed by individual departments, however, and were shaped by and around already existing city, regional, or state intelligence centers and communication infrastructure, the quality of relationships with the FBI, and localized political pressure on privacy and security concerns. The Suspicious Activity Reporting Initiative was launched in order to link these efforts into a nationwide system.

In the Miami-Dade region of Florida, the police department had been shocked by the knowledge that, as one local newspaper put it, "the 9/11 terrorists lived, trained and did business" in their county.[19] Prior to participating in the Evaluation Environment, the department had a directive on "Handling of Criminal Intelligence." They issued another directive, on reporting, before joining the pilot project, in late June 2008. For the official Evaluation Environment period, they decided that those two directives were sufficient and created no general or special order as part of their participation in testing the Suspicious Activity Reporting Initiative, although they did refine their vetting process. The procedures were as follows (abbreviated and lightly edited; US DOJ 2010b:128-129):

> Prior to the Evaluation Environment, Miami-Dade police officers' reports were submitted in hard copy to the department. If an officer determined that the report included suspicious activity, the report was forwarded to Miami-Dade Fusion Center (MDFC), which served as the collection point for all SARs from the department. Officers were also encouraged to call the fusion center to inform the center of the suspicious activity noted in their reports.
>
> During the ISE-SAR Evaluation Environment, the center developed a multilayer review and vetting process to identify SARs. Once the initial report is submitted by an officer, a field supervisor within the police department reviews the report to ensure accuracy and appropriateness. Sent to MDFC, it is immediately reviewed by an analyst and investigative personnel to determine its relationship to terrorism. If the SAR is credible, a detective will deploy to the scene for follow-up. Once the review is complete and analytical value added, the SAR is then reviewed and approved by an MDFC supervisor

> before entry into the ISE-SAR Shared Spaces.
>
> If an SAR is deemed to be credible, feedback is provided to the original submitter of the SAR and, depending on the validity of the information, commendations can be issued.

Central to the initial reporting is the police officer as the discerning subject. The technology of anticipation relies on the officer's management of uncertainty to produce the determination of suspicious activity. Likewise, once an encounter or incident report arrives at the fusion center, there is a set of skills applied to turning it into an official Suspicious Activity Report (SAR).

Suspicious Activity Reports

The ISE-SAR Initiative idealizes suspicious activities as self-realizing actualization: the terrorist's preoperational plans are unfolding, and the officer spots them. Yet such micro-incidents do not count as suspicious activity until they are identified as such, and, taken as a complete process, this is a matter of discernment, rather than technical detection. Efforts to discern the suspicious purely in behavior and context are confounded by the reality that these agents cannot perceive *with* discernment but *free* of their lived experience and shaping. The training offered to officers and analysts is a particularly important venue for making explicit or at least lessening the power of any faulty internalized guides, although often it does the opposite (cf. Stalcup and Craze 2011). Whether the capacity for discernment is shaped in counterterrorism training or everyday policing—also with well-documented biases—it is necessarily deployed and thus "directs" the actualization of potential uncertainty. Although this has many ramifications for the ways that security shapes life, what is pertinent here is how the system handles this inherent tendency to reproduce known or imaginable possibilities.

The Evaluation Environment final report optimistically sets out a four-part "integration/consolidation" process, which involves reviewing the activities to vet them for "a potential nexus to terrorism" after collection (US DOJ 2010b, 17). In practice, procedures for this vary from one fusion center to another. A concerted effort is made to specify any ties to terrorism, in a process that privileges the decision of the analyst, like the officer, in dealing with what is in hand. The lead analyst at one fusion center explained:

> I don't want a checklist. If I have an incident report, I have to look at it. Then maybe I will check three things that catch my attention. What I check is not always the first thing on the list. Let's say I look through one week's submitted reports—that [collection of

> reports] will tell me something, not the checklist. That will me give a sense of what is going on. Furthermore, it's intrusive to check the criminal database for someone, and I want to have a reason.

What is assessed, what counts as significant, and the analyst's sense of ethical comportment are brought to the fore.

After the analyst has done a preliminary check, the incident report would be reviewed at the fusion center's weekly meeting with analytic staff, and representatives from federal agencies not located in the fusion center, but one floor up, which might include the FBI, ICE. and US Marshals. The procedures would be recognizable to analysts elsewhere, even if not identical. Each incident being considered for submission to the networked "Shared Spaces" or federal intelligence databases would be presented by an analyst, together with supplementary information she had collected. At the meeting, the representatives would discuss the incident in relation to "what was happening" locally and according to intelligence sent from the federal level. Like the officers on the street, the analysts are supposed to become familiar with the local state of affairs such that they have "a sense" of what something indicates.

The intelligence team leader recounted how one analyst had been assigned an incident, and "started running the name down" through federal database systems. There was a link to criminal activity in the past, specifically, drug smuggling.

> We went back to the local police department, and asked for old intakes. There, we found linkages with drug criminal history. So, this just doesn't pass the smell test for terrorism. It seems like a smuggling ring. That was the question we asked at the meeting, "which vat does it go into?" What we can say is, based on our findings this is what we think it is. It should go to the police department, maybe DEA, or the gang unit.

For the officers and analysts, interaction with the uncertainty that intelligence gathering addresses is part of the subjectivity they must cultivate. Formal criteria tend to be eschewed by both. At the most basic level, the officer aims to distinguish between the ordinary and the suspicious, marking this distinction in the potential of undifferentiated moments of human life observed on the street or in an encounter. They practice discerning what "does and does not belong," and through that practice the virtual event becomes the suspicious incident in the register of observations and encounters. The analysts take this documentation, as well as calls and tips that make up their raw materials, and, in a sense, repeat the process as they decide what is to count. None of it is

meaningful per se; by the very norms of the analytic process the data are wiped clean of the significance attached by those who provided them—repotentialized—to be assessed. This is not to say that sources' authority and their prior assessment are unimportant. Who provided the information and why they did so are crucial points, not in and of themselves, but as criteria used by the analyst in the process of differentiating what is significant (suspicious) and what is not.

After Anticipation

An anticipatory technology, although it will multiply incidents, does not produce events. Incidents are, by design, meant to be detected in direct proportion to their independent manifestation. In relation to the bulk of those human activities that the police handle, or even criminal activities, they will be relatively few. A functional anticipatory technology will find mostly crime (unless there is much more terrorism activity in the United States than any evidence suggests). This explains the findings of a 2012 Senate committee that reviewed the fusion centers and their input into national intelligence. Attempts to assess the initiative's output by how much terrorism it found, as Congress hoped to do, were frustrated: "Most reporting was not about terrorists or possible terrorist plots, but about criminal activity, largely arrest reports pertaining to drug, cash or human smuggling" (HSGAC 2012, 2). The Senate committee also found:

> Nearly a third of all reports—188 out of 610—were never published for use within DHS and by other members of the intelligence community, often because they lacked any useful information, or potentially violated department guidelines meant to protect Americans' civil liberties or Privacy Act protections.

The committee was angry and also flummoxed by these results, although, dusty archives are presumably where reports *should* go that do not seem "reasonably indicative of pre-terrorism activity," if they are kept at all.

The documentation of incidents serves not to find a specific event but to hold the "time" of potential, and extend the period of the pre-event. Each traffic stop is an encounter with an unknown and unknowable future; the uncertainty, the virtual richness, of the interaction is preserved as it is turned into an official SAR, much as it had been preserved in the archives and databases of police departments. The potential is made

available in the system as data that can be repurposed, but no event past that point is necessarily suggested or diagnosed.

However, this is left to other technologies to take on. So while this basic level of national intelligence work retains and even increases potentiality, this phase does not extend into indefinite or infinite uncertainty. Suspicious activity reporting, in discerning the micro-instances that anticipate the event, is restrained and is generative as part of the broader intelligence assemblage. Evidently the process is not politically neutral or unconstrained, residing as it does in government databases for discerning threat. The official SAR channels incidents onto the path of "terrorism," albeit not in relation to a specific event. The intermediary role of suspicious activity reporting (its expansion of the "becoming period" prior to an event), means that it can equally feed technologies of prevention and preemption. Suspicious behaviors have long been documented at the street level, but once archived, these tended to be reactivated only in the event of a crime later on. The advent of intelligence-led predictive policing increased the routine use of suspicious encounters, but retained a tight linkage to crime incidents. SARs, however, can be decoupled from criminal matters, and thereby lend themselves more easily to the speculative (or fraudulent) construction of a preemptive case against someone. This may be on the basis of a different (non-criminal) profile. Surveillance of constitutionally protected activities have been found in the fusion centers of several states, suggesting that rights, and also the logic of anticipation (in which the goal is not simply more information but significant information) are challenged by the conflation of suspicion with behaviors.

Alternatively, still in a preemptive mode, if suspicious activities are linked to a subject, an agent provocateur can instigate what the FBI calls a sting operation, the "ultimate goal [of which] is to catch a suspect committing an overt criminal act such as pulling the proverbial trigger but on a dud weapon" (Bjelopera 2013). One informant described it this way:

> The only way to prosecute these guys is to give them every option to trap themselves. Yes, most of the time you're putting weapons in their hands. Otherwise all you can prove is that they had intent. If you don't provide capability, what can you do? If you do, you can get them in the act. An FBI agent can't go to a mosque to convert a group to radical views. But if you get a call from a parent, and you get turned onto someone that way, you can hear him say stuff. You say, "I'm going to see how far this guy is willing to go." I am going to ask the kid a bunch of times, "are you sure…?" but I've got to find out if he's

> going to act if he has the weapons. We are either in front of the event, and people will say "entrapment" or we are after. If we're after, the attack may have been successful.

Through the actions of the FBI, in nearly all cases since 9/11, an ensemble of incidents was preemptively provoked into a (highly controlled) event, subsequently charged as attempted terrorism. The Congressional Research Service (CRS) estimates that there have been 63 homegrown violent jihadist plots or attacks in the United States since September 11, 2001 (Bjelopera 2013).[20] Although an official count of terrorist sting operations is not publicly available, the FBI has said that of the terrorist plots disrupted between 9/11 and the September 2009 Zazi plot to bomb the New York City subway, two plotters were "prepared to move ahead with their plots without the benefit or knowledge of government informants or US officials" (Bjelopera 2013, 21).[21]

Conclusions

Among the "Lessons Learned" in the official report on the Evaluation Environment, two were particularly notable (US DOJ 2010b, 42). The first was that there was no clear agreement on what constituted a terrorism-related suspicious activity. The second was that none of the participants were sure how suspicious something needed to be to get classified as an SAR. The heart of this confusion was not the need for better guidelines or more details in any specific case, but the fact the initiative hoped to bring forth a discerning subject who would be able to differentiate a special kind of suspicion.

The architects of the initiative reasoned from their early insight about traffic stops with the soon-to-be 9/11 hijackers that officers had always collected and documented suspicious activities. Suspicious activity reporting was conceived of as an extension of everyday policing and criminal intelligence; the difference was in altering "suspicious" from a primary differentiation of potential uncertainty to instead indicate a category of possibilities related to terrorism. The common legal standard of "reasonable suspicion" required for questioning, stopping and searching someone was swapped out for "reasonably indicative of terrorism-related activity." Counterterrorism training was intended to enable whatever expansion of capacities was needed to discern that which might be a precursor to terrorism. Officers would keep themselves attuned for certain signs while they went about their routine patrol work. By accumulating suspicious incidents, located in the intermediate period that is the pre-event, the potential with which

the counterterrorism intelligence apparatus overall could work was increased (although those caught up in it were not necessarily terrorists).

The initiative was thus based on the demand to learn to recognize a specific category of behaviors (possible terrorism precursors), without this compromising the capacity to discern that which is simply outside the norm. In the face of this paradox, standards of officer and analyst performance had been set, but they had not been internalized by the subjects of performance, nor were they stable. As the trainer in Florida brought up, instructing officers to engage differently with uncertainty by looking for terrorism may distort their very capacity for discerning the suspicious. Nonetheless, police departments hoped to learn from their local fusion center what to look out for, such as timely information on a new fundraising scheme or plans to case a local transportation site, and therefore they were willing to participate.

Security, as a form of governance, is of course redesigned in an ongoing manner. Diverse logics undergird governmental practices that draw on and adapt to differently imagined futures, perceptions of crisis, scandals that impact public opinion, and shifts in jurisprudence. Discerning suspicion is only one way of handling uncertainty. Anticipation is only one event technology among many in use in security governance, and may yet be refashioned by more powerful technologies. Should capacities and practices cultivated in policing to deal with terrorism rather than uncertainty succeed in taking root, however, these may well continue, unmoored from the technologies themselves.

[1] See the "Complete 9/11 Timeline" at http://www.historycommons.org, an open-content investigative journalism project, on matters of fact not otherwise referenced throughout this chapter.

[2] I use the term "police" throughout this chapter to refer to the large range of sub-federal law enforcement in the United States, which includes city, county, state and tribal police; sheriff departments; and highway patrol, among others.

[3] I researched security practices among police and in parts of the intelligence community from 2006 through the beginning of 2014, conducting multisited fieldwork in the United States and at Interpol headquarters in France. I use pseudonyms to refer to all individuals with whom I spoke during fieldwork; additionally, some quotations were adapted to avoid revealing geographic location when it could identify the interviewee.

[4] Whereas previously a division was marked between foreign and domestic intelligence, "national intelligence" appeared as a significant term after 9/11. Thus, while the collection and use of intelligence was not new, its production was evolving, diversifying in type and institutional components.

[5] The FBI was simultaneously developing its capacity in domestic counterterrorism, including the eGuardian portal through which it could receive reports of suspicious activity directly from local officers and other government actors, such as the military. The Bureau wanted to assess and retain information for incorporation in its classified Guardian system. This suited some policing organizations, particularly those that did not have advanced intelligence capacity and did not want the added burden, but concerned others that wanted to retain control over information about citizens to whom they were accountable.

[6] On risk and prevention, see, for example, Beck 1992; Ericson and Haggerty 1997; Luhmann 1993; and O'Malley 2000. On preemption, see Amoore and De Goede 2008; Anderson 2010; de Goede and Randalls 2009; Ericson 2008; and Massumi 2007.

[7] As Macedo (2008: 9–10) differentiates, the "first and clearest case of just war is defensive: to defend against an unjust attacker and to secure the conditions of peace" but there is also "one additional narrow category of just war: preemptive war in response to a threat of attack that is not only overwhelming but also so imminent as to allow no time for deliberation and no choice of means."

[8] Policy commentators were duly observant. Macedo observed, "the Bush Doctrine of *prevention* [is] misleadingly labeled as 'preemption'" (2008, 10; italics in the original). A RAND publication noted that the Bush administration's redefinition of the term differed from "generations of scholars and policy-makers" (Mueller 2006, xi).

[9] François Ewald influentially analyzes precaution as stemming from the "uncertainty of scientific knowledge itself" (2002, 286). Prominent in European environmentalism, the precautionary principle has been explored as the justification for taking measures, despite lack of certainty, in the face of the threat of terrorism (cf. Aradau and van Munster 2007; de Goede and Randalls 2009; Stern and Weiner 2006). Preemption in this literature is differentiated by the way uncertainty is taken up and made to manifest.

[10] Notably, when these concern terrorism, intentionality is assumed and these are taken to be performative utterances endowed with great illocutionary force. See Austin, John L. 1962 [1955] *How to Do Things with Words.*

[11] When CVE shifts from addressing causes to intervening in how subjects to respond to them, however, potential reenters and uncertainty gains a positive valence, as "resilience" is built up in subjects perceived as vulnerable to radicalization.

[12] One version of "anticipatory action" is that it is enabled to work upon imaginations of the future (cf Anderson 2010). Also, Amoore (2011, 2013) describes how data derivatives are put to use in an anticipatory logic, which does not predict what will happen but projects the fragments as a way of rendering calculable possible futures. Here, I wish to distinguish a distinct anticipatory mode of uncertainty and Suspicious Activity Reporting as a technology that works in that mode.

[13] But see Hidek (2011, 247), who argues, "by claiming that state and local intelligence networks evolved from the 'bottom-up', those responsible for their birth and expansion (defence contractors supported by key federal officials) maintain the ability to carry out the work without informed oversight and regulation."

[14] See, for example, what is provided under "Background" by the Information Sharing Environment at ise.gov.

[15] Authorizing instruments include the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001; the Homeland Security Act of 2002; and the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA).

[16] These included the IACP, the National Sheriffs' Association, National Organization of Black Law Enforcement Executives, the Major Cities Chiefs Association, and the Police Foundation.

[17] This included by 2007, when fusion centers were being actively promoted by the federal government, five interconnected grant programs, (1) the State Homeland Security Program, (2) Urban Area Security Initiative (UASI), (3) the Law Enforcement Terrorism Prevention Program (LETPP), (4) the Metropolitan Medical Response System (MMRS), and (5) the Citizens Corp Program (CCP).

[18] Judeo-Christian tradition held that it was not possible to know God's mind, but that it was possible to discern the significance in our moment in history. Scholarship on discernment took a different turn with the work of Heidegger; the effect of the hermeneutic shift was a decoupling of discernment and history within these analyses. Discernment as a capacity developed by police officers, however, is linked to neither comprehensive history nor the universal/eternal, instead operating in, per Paul Rabinow (2011), a contemporary mode with attention to the historical aspects of the world, which are inescapable, as well as the distinctive forms of objects and life practices that are all around.

[19] "South Florida locations frequented by the 9-11 terrorists." *Sun Sentinal*, http://www.sun-sentinel.com/sfl-terrorists-florida-map,0,2619314.mapmashup.

[20] This excludes "foreigners largely radicalized abroad" and acts attributed to "violent extremists inspired by non-jihadist causes such as radical environmentalism, animal rights, or anti-abortion causes" but includes the "shoe bomber" Richard Reid (December 2001), the Transatlantic Airliners plot (August 2006),

the attempted airline bombing by Farouk Abdulmutallab (Christmas Day 2009), the Printer Cartridge plot (2010), or Quazi Mohammad Rezwanul Ahsan Nafis's attempt on the Federal Reserve Bank of New York (2012). See Bjelopera 2013, 1.

[21] Ten defendants charged with terrorism-related crimes formally, but unsuccessfully argued the entrapment defense in six trials between 9/11 and early December 2011. See Bjelopera 2013.