Abstract

What is at stake when citizens are encouraged to deploy vigilant surveillance and report what they consider to be unusual and “suspicious” activity? This article explores the current role of vigilance in contemporary Western security practices aimed at battling terrorist acts and major crime. It does so by critically analysing official constructions of suspiciousness, the responsibilisation process of participatory policing, and the assignments of prejudiced amateur detectives. It concludes, firstly, that the agency offered by political campaigns such as “If You See Something, Say Something” is highly illusive since the act of reporting simply demarcates where participation ends, and where fear and paranoia are turned into legitimate intelligence, enabling the state to exercise authoritative action and preemptive violence. Secondly, these kinds of vigilance initiatives also nurture a normalisation of suspicion towards strangers since the encouragements to be aware of anything-and-anyone deemed “out of the ordinary”, as well as the tools for reporting such suspicions, increasingly creep into the mundane realms of everyday life.

Introduction

This article explores how vigilance is called for and deployed as a surveillance technique in the reporting of “suspicious” activities and individuals in society. It analyses the implications of participatory policing initiatives in contemporary security work geared towards countering terrorism and major crime, where fear and suspicion have become integrated as techniques of governmentality. Through shifts in public responsibilities, ordinary citizens are encouraged to be vigilant in their everyday lives and engage in the monitoring of behaviour that is deemed “out of place” or “out of the ordinary”. Conceived as deviations in an otherwise normalised way of life, unusual patterns in society are supposed to be reported onwards to public authorities who manage risk and carry out preemptive strikes. As will be shown throughout the analysis, this kind of vigilance is today promoted most distinguishably within the frames of US “homeland security” campaigns, but also resonates strikingly with similar strategies in the UK, Australia, Canada, and elsewhere in Western societies.
As a type of surveillance drawing on various traits of “suspiciousness”, vigilance is somewhat understudied in its current configuration within security practices. Therefore, this article asks: what is at stake when citizens are encouraged to deploy vigilant surveillance and report what they consider to be unusual activity? How are notions of the “suspicious” officially formulated, and how are citizens engaged in the act of “reporting” it? By critically assessing how everyday social deviances become constructed as precursors to dangerous threats, especially in the context of participatory forms of policing, a wider problem is approached in how citizenship serves, if anything, as a fragile constitution in societies where a dominant security apparatus allows anything-and-anyone deemed “out of place” to transform into a potential threat. Security agencies do not simply ask to lend the eyes of citizens, but simultaneously draw on their perceptions, prejudices, and “gut feeling”, and deduce from this “evidence” for justifying authoritative action, and if necessary, preemptive violence.

This discussion will be initiated by engaging with Walter Benjamin’s reading of the concept of the flâneur as an urban amateur detective, and introduce this notion to more recent theorisations on participatory policing and the “surveillant gaze”. Since the scope of this article does not allow an exhaustive account of the wider workings and historical trajectory of vigilant citizenry, it will provide a critical account on recent societal (in)securitisation processes wherein everyday acts of vigilance are explicitly encouraged as a particular method of surveillance aiming at the “pre-incident” stage of crime and terrorism. To this end, an analysis will be laid out in two parts. The first part discusses how constructions of suspicions are positioned in relation to a normalised way of life by drawing on a discourse analysis of public reports, announcements, and strategic definitions provided by the Department of Homeland Security (DHS) and Nationwide Suspicious Activity Reporting Initiative (NSI), as well as vigilance campaigns such as “If You See Something, Say Something” which crosscut local, regional and governmental levels. These sources are indeed fragmentary of the otherwise vast universe of regulations and legislative acts forming the wider objectives of “homeland security”, however, as will be shown, they still resonate distinctively with how vigilant surveillance is set up and deployed in similar projects in e.g. the UK, Canada, and Australia.

Secondly, the analysis will turn towards the act of “reporting”, and thus, to a focus on the stakes involved in participatory policing. Stemming from a field of professionals, vigilant surveillance involves a plurality of relational, interconnected, competing, and incoherent (both public and private) actors, aiming generally for corresponding goals of “increasing” security (Bigo 2012a). When we speak of “security”, however, it is never a matter of what it means but rather of what it does; security is indeed “the name given to certain practices that might otherwise be called violence, coercion, fear, insecurity, freedom, mobility, or opportunity” (Bigo 2012b: 124). Any implementation of security will always create insecurity for others: this illustrates the tipping point of (in)security which balances the “normal” worthy of protection, against the “abnormal” subject to exclusion or transformation (ibid: 129; see also Balzacq et al. 2010; Bigo and Tsoukala 2008). Hence, the second part of the analysis will have to focus on the practices of reporting: where do reports end up after being uttered, with what tools are they transferred and received, and how are fears and suspicions subsequently operationalised? Critical findings on so-called “fusion centres” will be discussed, as will the way these kinds of instances of control rely on biased information from amateur detectives, and treat “reports” as perfectly legitimate evidence and justification for their actions. The dimension of proximity provided by reporting tools will also be illustrated by analysing how mobile technology is implemented within vigilance campaigns. Seemingly, the role of the “citizen-soldier” becomes increasingly accessible to perform in everyday life due to the proliferation of user-friendly smartphone applications, telephone hotlines, and social media channels.

However, as will be concluded, the current configuration of vigilant surveillance in many Western societies contributes to a normalisation and perpetuation of distrust towards strangers. Reporting-routines creep into everyday life without attracting too much attention, they slip into the mundane and unspectacular, and their serious implications become obscured by catch-phrases on billboards in the city, posters in the public transport system, in television advertisements, and so on. When a responsibilisation
process becomes increasingly trivial and accepted, reporting other human beings as potential threats to society and exposing them to the categorical violence of authoritative action demonstrates the mere symbolic value, and inherent fragility, of being a citizen.

“Soft” Surveillance? From Flânerie to the Surveillant Gaze

The type of sensory surveillance adopted when citizens monitor specific social (or typically, urban) settings will be conceptualised, firstly, by reflecting on the “amateur detective” found in Walter Benjamin’s The Arcades Project and adjacent pieces of work. Citing early literature on “idling and people-watching” (i.e. flânerie) in general, and the poems of Charles Baudelaire in particular, Benjamin gradually sketches out his take on the notion of flâneur. This urban stroller who “botanized on the asphalt” was both a literary character of the 1840s panoramic “physiologies” genre, as well as a common sight in the commercial arcades of 19th century Paris, a city which was transforming into a “labyrinth of commodities” at the time (Benjamin 2006: 68, 85). The term flâneur itself carries several connotations and characteristics: it signifies the observer of the marketplace, the explorer of the city, the connoisseur of the street, the autonomous spectator of an urban scenery. The flâneur does not challenge such sceneries, but rather embraces them, lives through them, and devotes itself to the pulse of street life. It thinks of the city centre both as an arena and theatrical display, as well as its own dwelling place where pretty house facades and enamelled shop signs evoke a sense of “home”.

In Benjamin’s definition, the flâneur is always in full possession of its own individuality, and is thus distinctively different from the badaud (a person in the crowd, the bystander and “gawker”). In fact, the crowd serves merely as a veil behind which the urban explorer seeks refuge, for the flâneur is an optical rather than tactile agent, a curious and autonomous agent of surveillance who hides within crowds in the streets, keenly gathering the visual data emerging before its eyes and filtering it through lived experiences (Benjamin 2002: 206-207, 417). The badaud on the other hand is “absorbed by the outside world”, becomes intoxicated “under the influence of the spectacle which appears before him”, and morphs into the impersonal creature of the crowd (Benjamin 2006: 248-249). According to Forth (2004: 107) “the badaud walks for the sake of walking, is amused with everything, is captivated by everything indistinctly, laughs without reason and gazes without seeing”.

The flâneur, in sharp contrast, applies a purposeful gaze and regards itself as being “on assignment in the realm of consumers” (Benjamin 2002: 427). An inherent element of Benjamin’s figure is that of being a “detective”: this is the “social legitimation of his habitus”, the appropriate and plausible “front” for being the watchful observer “who will not let the unsuspecting malefactor out of his sight” (ibid: 442). Benjamin echoes the contemporary socio-political setting as well: “In times of terror, when everyone is something of a conspirator, everybody will be in the position of having to play detective”, and as such, the flâneur does not glorify the criminal or the suspect, but does rather “glorify his adversaries and, above all, the hunting grounds where they pursue him” (Benjamin 2006: 72). Per definition, the amateur detective will indeed always be one of the “watchers”, rather than the stranger who becomes watched under suspicion.

The Arcades Project is a fragmentary outlook on Parisian urban life; an unfinished compilation of quotes, notes, and aphorisms. Nevertheless, the flâneur still comes forth as a compelling figurative component of Benjamin’s critique on modernist society: it is the alienated urban dweller who “takes pleasure in abandoning himself to the artificial world of high capitalist civilization” (Lauster 2007: 140). By possessing privileges unavailable to “gawkers”, the flâneur can be simultaneously tangled up in urban life (performing the detective role of monitoring otherwise overlooked patterns and persons) and wholly detached from it (acting autonomously from faceless crowds). In a sense, this character is able to signify the archetype of the liberal dream; it is in full possession of its sovereignty in the streets, it is a “prince who everywhere rejoices in his incognito”, to use Baudelaire’s own words (cited in Benjamin 2002: 443).
Strolling the streets as an amateur detective is indeed a privilege made available only to some, and vigilance is to Benjamin’s figure associated with freedom rather than notions of “responsibility” and “duty”. However, these latter elements are of central importance if we turn to more recent work on so-called “soft” surveillance, according to which an amateur detective could be assumed to apply a vigilant gaze out of compliance rather than choice. “Soft” surveillance resonates somewhat with the scenery of the flâneur since it, too, entails the monitoring of everyday life and the surveillance of various everyday sites of social interaction (urban spaces, consumption, leisure, public transport, and so on). By taking place in the mundane and unspectacular realms of society, much of the controversies typically entailing surveillance practices are avoided. Often deployed in crime prevention, this is also a type of “participatory” surveillance which frequently relies on public engagement the population and expects citizens to “play along” in some of its methods, for example, by lending their eyes and ears to law enforcement agencies (Haggerty 2012; Lyon 2007: 36). This is thus distinctively dissimilar from “hard” surveillance (e.g. monitoring inmates in maximum-security prisons) wherein there is clear differentiation between watcher and watched, and where watching people is often coupled with disciplinary methods of control and use of force in the expectation of heavy resistance.

This development towards a responsibilisation of citizens is a driving force in what has been called a “reinvention of liberal governance” (Hay and Andrejevic 2006: 342; see also Garland 2001: 124; Zedner 2009: 77). The implementation of participation in surveillance and policing is indicative of how security agencies today are striving for universal, or at least increased, “inclusiveness” in the safe-guarding of a community (Marx 2006: 37). Surveillance might even become “welcomed as an ally, an alibi or an ark” by some according to the logic of if you are innocent, you’ve got nothing to fear (Lyon 2007: 163).

The flâneur, once an amateur detective out of simple pleasure, is in today’s political scenery instead confronted with expectations of what it entails to be a “good” citizen. Its eyes and ears become political participants and serve as extensions and embodiments of security institutions. When partaking in the detective work of monitoring societies for unusual patterns and behaviours, citizens must adopt with their very own senses what Gary Marx (1989) has called a “surveillant gaze”: a way of watching that has its historical roots in the profession of policing and crime-fighting, used as a tool in the patrolling of communities for sorting out that which is deemed “out of place”. This way of gazing is often expanded from a sovereign to the population, as most initiatives stem from a single agent (e.g. an authority), but are carried on further by a plurality of subjects (e.g. citizens). Consequently, citizens can also “watch each other” (Ball et al. 2012: xxvi), or engage in what is called “mutual monitoring” within societies (as a complement to centralised monitoring) (Andrejevic 2006). This way of watching presents the citizen with certain duties to protect and serve: Haggerty (2012: 236) notes that when “officials encourage individual citizens to conduct their own anti-crime surveillance”, policing as a method is no longer restricted to the public police force. Andrejevic (2006: 450-451) calls this a “capillary extension of surveillance into households and surrounding neighbourhoods” wherein law enforcement put trust in the “plain old gut” and “trustworthy instincts of the good citizen”. With these developments of vigilant surveillance and participatory policing, it seems as if the perceptions of the flâneur are increasingly merged with the professional regimes of security work.

In a cultural study, John McGrath illustrates how this gradual handover of duties is something many citizens have begun to embrace rather than resist, pointing towards TV shows such as Crimewatch UK. Herein, it is stated that “your call could be all it takes to put an offender behind bars” as the police force claims to be in need of the public’s help in order to identify criminals. The entire concept revolves around the proposed benefits of extending a surveillant gaze via the audience: “Police officers solemnly thank viewers for their help in bringing criminals to justice. The whole show is based upon the recognition of criminality: ‘Do you recognize this man?’ is its constantly repeated refrain” (McGrath 2004: 29). By playing along with the logic of if you are innocent, you’ve got nothing to fear, the viewer is “reassured
that his or her image has been sorted through and passed as law-abiding and therefore does not need to be circulated” in the television crime shows (ibid: 168).

Two caveats must be presented for the theoretical framework sketched out above. First, “soft” surveillance is a rather deceptive analytical definition. Distinguishing between soft and hard surveillance methods, implying that some are “less” privacy-infringing or “less” violence-enabling than others, is dangerously misleading. This distinction deflects attention from the (in no way “soft”) security practices that become legitimised and justified, for example, by the reporting of suspicious behaviour by vigilant members of the public. Instead of undermining the implications of some types of surveillance, it is precisely their enabling of categorical violence that should be highlighted.

Second, and related, the urge to interpret certain forms of surveillance as “mutual monitoring” can also be contested. The claim is that mutual monitoring, as a component of participatory policing, is a way for citizens to “increase security” by both watching each other and the everyday work of law enforcers. Instead, one should rather view these participants as together postulating a sense of “normality” reinforcing a symbolic and cherished way of life, which in turn opposes unwanted suspects. Only certain appearances and behavioural patterns will become reported as “out of the ordinary”, and individuals behind this veil of distrust will indeed have a hard time “participating” in securing anything once they become deemed potential threats and mere action-points for authoritative force. The privilege inherent in the flâneur is sustained: only a privileged few get to be watchers, i.e. those who comply with authority, agree to play the reporting-game, and “fit in” as usual and ordinary elements of society.

**Current Regimes of Vigilance and Suspicion**

In the US, a shift in responsibility is noted in statements such as “homeland security starts with hometown security”, and in assuming that certain activities preceding disastrous events “might be observable and reportable by a vigilant member of the public” (DHS 2015a). Hay and Andrejevic (2006: 336) have discussed elsewhere that this signifies how homeland (in)security is increasingly becoming an “experimental” enterprise where civil society is viewed as both an “object and resource”. A strike of terror, for instance, could implicate the civil society not just as collateral damage, but also as primary targets, and citizens are thus required to stay well-informed and in a state of readiness. This points towards a militarisation of domestic security practise in how state agencies mobilise citizens as “soldier[s] in a state of perpetual vigilance” (ibid: 341), indeed, as a form of first line of defence. Governments withdraw to a supportive role and simply “offload duties” onto individuals, spawning citizen-soldiers who are to be on the qui vive for attack, ready to participate in the so-called war on terror from the privacy of their homes, from their workplaces, and during their spare time.

A compelling example of this development within homeland (in)security is traceable to when the Nationwide Suspicious Activity Reporting Initiative (NSI) initiated its operations in 2010, resulting in the deployment of nation-wide vigilance campaigns named “If You See Something, Say Something”.¹ Fronted by the departments of Homeland Security and Justice respectively, these campaigns are carried out operationally by the law enforcement and a range of state-level transportation organisations,

---

¹ The now internationally recognised vigilante catchphrase “If You See Something, Say Something” was originally coined by adman and “tag-line expert” Allen Kay of Korey Kay & Partners in the aftermath of 9/11. The slogan was pitched to one of KK&P’s long-term partners, namely the New York Metropolitan Transportation Authority, subsequently resulting in an advertisement campaign in buses and subways throughout the city. Rolled out in 2003, the campaign cost around $3 million yearly which was paid to a large amount by the DHS (Fernandez 2010). The MTA later obtained full ownership of the slogan, and decided to license it out worldwide without charge for purposes of public safety. This specific campaign has been recognised elsewhere as an example of “the power of good advertising” (Wheaton 2010).
coordinated regionally via so-called “fusion centres” (to which I will return) (NSI 2014a, 2014b; DOJ 2006, 2008). Essentially similar strategies for citizen-participation in police work, including the reporting of “suspicions”, have also emerged in other Western societies in recent years. These related initiatives tend to apply the very same terminology, address similar issues, and deploy similar techniques of vigilant surveillance.

Vigilance calls aim at the “pre-incident” stage and are packaged as more or less harmless “campaigns”, “projects” or “programs” promoted as “simple and effective [ways] to raise public awareness of indicators of terrorism and violent crime” (NSI 2012a). This way, vigilance is advertised and made available to the public like any another commodity of security. To Andrejevic (2006: 442), it does not come as a surprise that US readiness campaigns, for example, are driven by a “market-oriented-solution mentality” and become “sold to the public via an advertising campaign, complete with focus groups, and, in one early proposal, celebrity spokespeople”. These campaigns are generally easy to grasp and interact with, and seek to induce a sense of contributing simultaneously to one’s personal safety and the greater good of society; for instance, the former DHS secretary Thomas J. Ridge finds vigilance campaigns to be “a very good charge for the American citizen” (Courson 2011).

In fact, both “community” and “individuality” play fundamental roles in recent calls for vigilance, and the contemporary flâneur seems to, again, be both tangled up in and autonomous from the everyday ongoings of urban life. Firstly, amateur detectives are posed as essential parts of the community wherein “we all have a role to play” according to US authorities, and by “working together, we can all help secure our country” (DHS 2015a). Secondly, in contrast, when the state of Georgia is told to “get ready” and protect itself, televised commercials repeatedly state how “one person can make a difference, and that person is you” (Ready Georgia 2010). It becomes apparent, again, that this duality rests on compliance rather than choice since the explicit political aim is to build “communities of trust” which are to facilitate improved understanding and cooperation between citizens and law enforcement in preventing crime and terrorism (NSI 2014c). In a similar effort, the London Metropolitan Police (2016) claims to “need the support and confidence of communities to improve the two-way flow of information in order to arrest and prosecute terrorists” since, apparently, “[c]ommunities can defeat terrorism”.

In detail, vigilant citizens are told to look for a range of specific indicators and signs preceding terrorist acts. Terror is planned and rarely spontaneous, authorities claim, and by looking for the correct “precursory activities”, violent acts can be exposed prematurely. “Terrorists have a lot of work to do before they attack” the London Metropolitan Police states (ibid), and this is echoed by the DHS (2015a): “Before they strike, many terrorists watch and study their targets, gather information, test security, acquire funds and supplies often through criminal activity, and rehearse or walk through their plans”. Through “tools” (i.e. standardised bullet point checklists) provided by the NSI, official analysts and investigators are able to pin down a caricatured definition of the “suspicious”, making individuals and behaviours actionable within practices of homeland (in)security. Careful attention should be paid to people who are:

- Questioning individuals at a level beyond mere curiosity about particular facets of a facility’s or building’s purpose, operations, security procedures
- Taking pictures or video of facilities, buildings, or infrastructure in a manner that would arouse suspicion in a reasonable person
- Demonstrating unusual interest in facilities, buildings, or infrastructure beyond mere casual interest
- Acquisition of unusual quantities of precursor materials, such as cell phones, pagers, fuel, and timers
- Attempts to obtain or conduct training in security concepts (military weapons or tactics) or other unusual capabilities. (NSI 2014d [emphasis added])
In London, the police encourage citizens to look specifically for material signifiers of criminal activity: vans, multiple passports, pay-as-you-go mobile phones, large or unusual quantities of chemicals, masks and goggles, suspicious use of cheques and credit cards, travel suitcases, padlocks to garages and sheds; that which “is probably nothing” but is still somehow worth reporting. Overall, vigilantes are often required to monitor the private and personal domains of other individuals’ lives, as illustrated by the Australian government (2015) who deem people suspicious if they simply have “a lifestyle that doesn’t add up”. This is detailed further by the Canadian police forces (RCMP 2010) who promote heightened attention towards individuals with:

- Visible anxiety when discussing themselves or when speaking to authority figures
- Living in a house with few furnishings/sudden surge in tenants
- Tendency to seclusion/no contact with neighbours
- Unusually high security for residential location
- Arrivals and departures at odd hours
- Visitors arriving/departing through garage or visibly obscured areas

Lastly, the British Safer Travel Partnership’s “See Something, Say Something” campaign refers to the related yet more ambiguous definition of “anti-social behaviour” fetched from the UK Crime and Disorder Act 1998. This definition encompasses “behaviour which causes, or is likely to cause harassment, alarm or distress to one or more persons” (Safer Travel 2015a).

Taken together, we can conclude that by aiming directly towards the suspicious and anti-social, by determining the unusual or that which is simply beyond mere curiosity or interest, what emerges at the same time is a fetishised notion of the “socially acceptable”, the “reasonable” and the “normal”. In fact, vigilance relies upon “the rational screening of normality in order to identify transgression” (Amoore 2007: 226). As exemplified by UK authorities: “Have you noticed activity where you live which is not the norm? We want people to have the confidence to trust their instincts” (Metropolitan Police 2016 [emphasis added]). The type of vigilant surveillance practiced today is thus not simply trying to unveil something “suspicious”, but is even more about continuously framing a given set of societal norms, and about postulating the rules within a certain cherished way of life.

In this process, not just individuals and behaviour are involved, but objects as well: in an Orange County spin-off campaign associated with “If You See Something, Say Something”, a several metres tall construction of a red backpack toured around the state as an advertisement installation to further spread awareness of the call to report suspicious activity. Standing in selected public spaces, such as town squares or crowded streets, “it is designed to draw their attention, to the real, larger issue of public safety”. A citizen comments: “A lot of times, you know, it won’t be that big, but […] we don’t think about that, we just want to carry on with our day” (Keep OC Safe 2013). When it comes to gazing upon objects that are deemed “out of place” it becomes a matter of singling out “from the cacophony of background noise in public spaces, that which demands a closer look, that which is out of the ordinary” (Amoore 2009: 19). Put differently, objects with a “spatial and temporal inadequacy” are simply in the wrong place, at the wrong time (Aradau and van Munster 2011: 97). Such objects can indeed be signified by the “unattended bag” (dropped off at a train station, containing explosives), an archetypical example of a potential hazard in public environments, warned against via PA system at train stations and airports throughout the world.

Sometimes, however, the object rendered “out of place” is seen as far more ambiguous and unknowable: In TV-broadcasted advertisements calling for vigilance in Connecticut, the suspicious object is depicted as a large, red, three-dimensional sign saying literally “SOMETHING” in bold upper-case letters (Figure 1). From a first-person view, this “object” is then spotted in mundane urban environments—on a bus, in a shopping mall, under a car in a public garage, at a train platform, etc.—representing that “SOMETHING”-object which citizens are supposed to report (ConnDOT 2014). This is rather remarkable stylistic gimmick.
Larsson: A First Line of Defence?

in which the eyes of the *flâneur* are appropriated and broadcasted by propagators of vigilance. Putting the amateur detective in its “natural habitat”, that is, “on assignment in the realm of consumers”, in the everyday settings of the city, the TV-set transmits directly the traits and techniques of an urban vigilante. Public spaces of the city are thus, with the assistance of the modern *flâneur*-figure, set up visually as both “vectors of attack” and a means for coordinating a distributed defence through the recruitment of citizen-soldiers (Hay and Andrejevic 2006: 341).

Furthermore, in public service announcements and via social media hashtags, the DHS regularly addresses the US national sports leagues that attract tens of thousands of spectators per each game, putting in increased effort ahead of and during mega-events such as the annual Super Bowl (Napolitano 2012). In video announcements showed on arena media cubes during intermissions, referees in the respective sports are depicted, about to enter the arena and start the game, proclaiming to the audience: “I pay attention for a living, I watch plays and make important calls. While I am busy watching the game, I need your help keeping an eye on the stands” (DHS 2015b). These calls for vigilance (by referees who also constitute the “authority” within the social universe of sports) do simultaneously frame a collectively enjoyed social life, as well as put its fate in the hands of the *flâneur* who must be alert in the scenery of gawking crowds. As potential disasters are brought into the cultural realms of entertainment and leisure, Salter (2008: 241) points out that the imaginaries evoked by these campaigns could be analysed “for their ideological meaning, as symptoms of broader sociopolitical trends, rather than intentional pieces of propaganda”.

Returning to Amoore (2007), she views the rise of vigilance calls as an emergent “watchful politics” wherein citizens visualise a “source of terror”, render it recognisable, designate it to specific people around them by drawing on xenophobic preconceptions, and similarly assume that “we” are normal and act normally. Racial stereotypization and categorical discrimination of “ethnic minorities” are major pitfalls when the visualisation of inherent fears becomes a task for an unsuspected majority. This is something security agencies tend to recognise and naively warn against: “Reporting suspicious activity should not be based on a person’s race, religion or gender, but rather on behaviours that seem suspicious

*Figure 1: A suspicious object (ConnDOT 2016).*
Larsson: A First Line of Defence?

or out of the ordinary”, the DHS (2015a) states. Profiling, recognised as an “actuarial method” within the police force where “criminal likelihood” is determined by certain characteristics and patterns of a category of humans, has been proved flawed and deeply destructive of social trust (Harcourt 2007). Yet, here, the hazards of profiling are offloaded onto the public together with the duty to be vigilant—although with the crucial difference that an untrained flâneur, as apart from law enforcement, lacks accountability and is able (and even encouraged) to report whatever prejudices he or she designates onto people and patterns deemed “out of the ordinary”.

**Reporting and Operationalising Suspicions**

Following the lead from the furiously repeated campaign narrative, as far as one has seen something, the following step is to say something. For this purpose, a number of tools are available. For non-emergency reporting, various channels are available throughout Western societies including “anti-terrorist hotlines”, text messaging services, and online reporting forms. Authorities in numerous US states have also ordered and rolled out a set of sophisticated and user-friendly smartphone applications developed by programmers in the private sector. In these “See Say” applications, smartphone users (who become “comfortably empowered”) can type in their report of the suspicious activity (anonymously or not), capture an image (“to ensure discretion, the camera flash is automatically disabled”), and submit it directly to local authorities. Via GPS technology and integrated maps, it also possible to pinpoint a precise location of the object, person, or incident in question. The chief of the Police Department in Boston concludes: “The ability to send in a photo or simply a comment directly to our dispatch center greatly enhances our ability to respond appropriately” (ELERTS 2015a). In user instructions in some of these applications, further characteristics of suspiciousness are added, such as odours and fluids, groups operating in an “orchestrated or rehearsed manner”, and people in “bulky” or “inappropriate” clothing.

Proximity is a key factor in these reporting-technologies since the gap between a threatening event and the ability to report it shrinks significantly. Soft surveillance becomes even “softer”; it becomes mobile, personal, and “smart” as programmers seek to turn applications into a link between the “eyes and ears on the ground” and emergency responders in the office. For example, another application is marketed for students and teachers to be used in the event of a school shooting, and includes functions not for reporting the criminal act per se, but for pinpointing one’s geographical position together with an “I am OK” or “I need HELP” message. Other solutions which similarly thrive on the “human-detection of threats” are offered to corporate security staff who, in the event of an attack or major accident, can take control over CCTV systems and activate a lockdown of their facilities, integrating distress calls with the building’s access control system simply by using a mobile touchscreen. The particular private tech-company cited here even had their mobile solutions tested by the US Federal Emergency Management Agency who rated them compliant with official emergency protocol standards (ELERTS 2015b). Critically, however, this entire technology is cloud-based, and since the cloud of data is owned and controlled by the company, they also hold the key to linking the actual incidents with the public first responders. In other words, this is a private enterprise built on profiting from insecurities by setting up and selling a technological commodity which serves as a gatekeeper to emergency response. This link between the supply and demand of security technologies (that is, the relationship between profit for some and disasters for others) is an example of the inherent problematique in the increased hybridisation in recent years between public and private domains of security professionals (Neocleous 2007; Larner 2008).

Today, “the post-crime logic of criminal justice is increasingly overshadowed by the pre-crime logic of security” wherein vigilant surveillance serves as but one among many measures of risk management, prevention, and preemption (Zedner 2009: 73; see also Anderson 2010; De Goede 2008). The act of reporting bridges the immediate future with preemptive action in the present, and it is many times the individual citizen, the privileged flâneur, who decides upon the fate of strangers by sending them into the
machinery of authoritative action. However, the actual agency which vigilance campaigns are suggestive of transferring to citizens is highly illusive:

It is not easy to put all the pieces together, and we don’t expect you to. That is the job of law enforcement and intelligence analysts [...] Never take unnecessary risks or try to act as an official investigator when observing or reporting what you have seen. (DHS 2015a)

When seeing something and saying something, it is first of all to be taken for granted that there are actually “pieces” to put together, however, citizens are not supposed to see the terrorist or the act of terrorism, but are rather instructed to spot signs or shades of a terror yet to come. The true “duty” is to simply anticipate and expect an approaching threat, never to actively engage with or stop it. As emphasised in the Orange County campaign, “[m]ost importantly, DO NOT take direct action, confront anyone, reveal your suspicions or touch an object. Just contact the authorities” (Keep OC Safe 2014). This marks an important boundary between the curious vigilantes and the sovereign state, with its “official” detectives of public agencies: in what is claimed to be a “shared effort”, the reporting-act functions as a mere delimitation for where vigilant surveillance ends, and preemptive action begin. The sovereign may become aided by the combined prejudice and paranoia internalised in the flâneur, but has itself retained the final power to exercise top-down violence.

How is authoritative action legitimised and organised? In the US, reports are sent to so-called “fusion centres” wherein security agencies from federal to local levels have partnered up to collect and share data with the aim of battling terror and crime (NSI 2012b; Monahan and Palmer 2009). In early attempts of regional intelligence-sharing efforts, the first centres that were established reminisced “silos of information” incapable of exchanging information swiftly, therefore, federal strategies were set up during the mid-2000s so that future centres working under the label of homeland security could be formed around a “fusion process”. In such a process, the aim is to produce “actionable knowledge” by enhancing coordination efforts between different actors, strengthening partnerships, and operating consistently with crime-fighting and antiterrorism efforts (DOJ 2006: 1-3). This allows for a collaboration (not just made possible, but preferred as ideal) where “non-traditional collectors of intelligence” (i.e. citizens and private companies) can be “fused” with law enforcement. (ibid: 20; DJS 2008: 18). When the NSI was subsequently implemented into the structure of fusion centres, it played a key role in tying together this cluster of agencies and actors with standardised procedures for observing, documenting, and investigating, specifically, “suspicious activity”.

Today, fusion centres operate in all US states and major urban areas and involve personnel from police departments, the DHS and DOJ, the FBI Joint Terrorism Task Forces, other public safety and transportation organisations, as well as private sector entities. This cluster of actors engages in “investigations of individuals, conduct threat assessments of events, identify patterns of criminal or terrorist activity”. Moreover, fusion centres can coordinate emergency responses, hold interrogations, and construct digital profiles of suspects (Monahan 2012: 287). In effect, the submitted reports of suspicions become merged and matched with digital profiles in databases. Via computers, authorities are able to gain direct access to local CCTV camera footage, and can even take control over unmanned aerial vehicles (or “drones”) in a given area. In short, the fusion centres have the capability to exploit virtually all of the technological features involved in the domestic war against terrorism in the US (ibid; DOJ 2008).

These fusion centres, which quite literally become what Didier Bigo (2002) has called “managers of unease”, have emerged as sites where suspicion and fear become institutionalised into a legitimate form of intelligence. The fusion centres are currently configured so as to drain the flâneur of its visual data and lived experience, run it through symbolic NSI frameworks, “fuse” it with official intelligence, and eventually transform it into organised practice. Injected with reports, either from citizens or law enforcers or via the clouds of private companies, these are clusters of interactivity where a range of (in)security
professionals conduct their everyday work. A flow of citizen-reports thus reaches the point at which it is decided whether or not the information is valuable, and if so, bottom-up surveillance can legitimately turn into top-down violence.

Elsewhere in the world where vigilant surveillance is at work, such as in Canada and the UK, coordinative efforts are typically associated with the respective police organisations, rather than particular domestic security centres or similar nodes of governmentality. However, a regional venture in London called Project Griffin (2012) serves as an exception since it is a joint private-public guild in which the “police, business and private sector security industry join forces to protect our communities from terrorism, extremism and crime”. Since 2004, this project engages with large organisations and businesses, and defines as its “primary role” to spread awareness, promote surveillance, and “[e]mpower people to report suspicious activity and behavior” (Project Griffin 2012).

Another interesting example from the UK, briefly mentioned earlier, is the Safer Travel Partnership which consists of regional police and public transport organisations, aiming to diminish anxieties and fears on British train networks by reducing “anti-social behaviour” in favour of a socially comfortable and “nuisance-free” environment. It does so, in part, by working with traditional policing and crime prevention, and in part by deploying a vigilance campaign with the very same rhetoric and technique as its NSI sibling. Reports are fed into an anti-social behaviour case management system called "ReACT" together with CCTV material and verbal statements (Safer Travel 2015a; 2015b). However, the partnership adopts a more informative and educational (or, if you will, biopolitical) role since it also provides youth workshops on public safety in schools across the country. Via teaching resources, class discussion topics, dramatic scenario enactments, role-playing, and more, a notion of socially “correct” behaviour is brought into the sphere of education. In effect, British pupils of a young age are expected to become deterred from a criminal lifestyle, while watchfulness is introduced as a comforting addition to travelling, and as a helpful way of aiding in police work. Arguably, vigilance among youngsters is hereby tied to the biopoliticised project of dealing with crime, seeking broadly to “sort out” the unwanted elements of social life (not just in transportation and commuting) and to mould knowledge of what is acceptable in a healthy and compliant society. As already noted by McGrath, these educational interventions seem fruitful in the UK population (and indeed elsewhere) given the popularity of interactive TV crime shows, and the size of not-for-profit organisations such as CrimeStoppers which provides services for civil society to anonymously report criminals and suspects. In these examples, instead of violence preemption, a more widely applicable societal precaution seems to be the guiding logic. Vigilance based on a precautionary logic relies on the assumption that everyone, indistinguishably and without evidence, is guilty at least of criminal intent. Precautionary surveillance thus directs attention to the vague and ambiguous, that which might become out of the ordinary, even if it is impossible to know exactly what type of threat might emerge from it (Ericson 2008: 57; see also Zedner 2009: 83).

**Conclusion: On the Normalisation of Distrust**

Vigilance, as a distinguishable human phenomenon, cannot be fully grasped by looking strictly at recent strategies for securing the “homeland” in the so-called war on terror, or at specific policing tools for regulating the socially (un)acceptable. Rather, understanding it holistically would require an extended genealogical study in which it would be possible to elaborate on vigilance as a transforming practice with long socio-political and historical trajectories. Indeed, vigilance appears to be driven by a range of interconnected factors: not just fear and suspicion in general, but governmentality, law and order, public awareness, community spirit, personal prestige, and economic profit. A genealogy of vigilance would also be able to elaborate further on the transition process (only mentioned in passing here) when the flâneur started to gaze over city life out of compliance instead of pleasure. It could be analysed, as well, to what extent the privileges of an amateur detective have evolved (or not), that is, what it has meant over time to
be able to avoid suspicion or particular interest, and rather become “the one who watches” alongside authorities.

Nevertheless, what has been found in the stricter scope of this article is the way in which participatory policing is at work today, how vigilant surveillance reports are deployed in security work, and in fact, how it seems like these matters of concern are becoming increasingly normalised elements in Western societies. As shown, vigilant surveillance takes not necessarily a “soft” but a mundane form and is practiced in many unspectacular realms of everyday life. The Met in London, for example, encourages people to find their suspicions in “nothings”:

> You may feel it’s probably nothing, but unless you trust your instincts and tell us we won’t be able to judge whether the information you have is important or not. Remember, no piece of information is considered too small or insignificant. (Metropolitan Police 2016)

Statements like these in fact resonate compellingly with what Huysmans has referred to as “little security nothings”. Simply keeping an eye out for someone or something is posed as a banal and harmless task, and so, watchfulness should be viewed as one of those security practices that are “strongly embedded in everyday actions and relations”, that progressively “slip into daily life without much ado” (Huysmans 2011: 377). Ordinary objects (a letter, backpack, parked van) become objects of danger, and the ordinary circulation of strangers in public spaces becomes, itself, a carrier of risk. This message is transmitted in similarly ordinary environments of everyday life: through a poster in the subway train, a billboard next to the highway, a speaker voice during the hockey game intermission, a commercial on the TV, an icon on the smartphone screen, and so on.

Understood as a little security nothing, vigilant surveillance is also a practice which is put in place relatively unnoticed via a myriad of decisions, work strategies, administrative moves, marketing plans, and so on. It is an ongoing, evolving, largely unquestioned and often obscured process, rather than a single, exceptional, rupturing “event”. This favours particular professionals of security since it allows them to spread their routines across sectors and geographical spaces without receiving much attention. Security practices are thus folded into the realms of everyday life, and participatory policing grows into a routiniséd practice of assembling the prejudices of amateur detectives, precisely as in the example of fusion centres.

This process is contributing to a routinisation of vigilant surveillance wherein its consequences are gradually blurred out. The responsibilisation move urges citizens to recognise suspicions not out of privilege or mere compliance, but out of acceptance and willingness as well. As a type of surveillance posed as “indispensable for everyday life”, it produces under the surface consequences that are “at least undesirable if not downright damaging” for solidarity between individuals and communities (Lyon 2010: 336). For example, when the notion of a “community of trust” is founded on the call for increased watchfulness and suspicion, in other words, the more “trust” becomes a matter of spilling information on others, participatory policing “leaves the social dimension vulnerable to erosion” (Lyon 2007: 116). In what Bauman would describe as “liquid” societies, vigilant surveillance is normalised, and expressions of distrust toward strangers have now “acquired a momentum of their own” (Bauman 2005: 69). Fear has settled within societies, “saturating our daily routines; it hardly needs further stimuli from outside” (Bauman 2007: 9). Indeed, this is a politicised process, one of weighing the usual against the unusual, of extending this enterprise to the public, and of turning collective prejudices into organised security practice. And to make this type of governmentality work, propagations to see something and say something must be based precisely on the mundane and banal aspects of everyday life, alas, resulting in a gradual perpetuation of fear and suspicion.
References


