Crowdsourced Countersurveillance: A Countersurveillant Assemblage?

Mark A. Wood
University of Melbourne, Australia
mark.wood@unimelb.edu.au

Chrissy Thompson
University of Melbourne, Australia
c.thompson7@student.unimelb.edu.au

Abstract

Speed camera ‘traps’, random breath testing (RBT) stations, and other forms of mobile traffic surveillance have long been circumvented by motorists. However, as technologies for traffic surveillance have developed, so too have technologies enabling individuals to monitor and countersurveil these measures. One of the most recent forms of these countersurveillance platforms can be found on Facebook, where dedicated regional and national RBT and ‘police presence’ pages publicly post the locations of various forms of police surveillance in real time. In this article, we argue that Facebook RBT pages exemplify a new form of social media facilitated countersurveillance we term crowdsourced countersurveillance: the use of knowledge-discovery and management crowdsourcing to facilitate surveillance discovery, avoidance, and countersurveillance. Crowdsourced countersurveillance, we argue, represents a form of countersurveillant assemblage: an ensemble of individuals, technologies, and data flows that, more than the sum of their parts, function together to neutralize surveillance measures. Facilitated by affordances for crowdsourcing, aggregating, and crowdmapping geographical data information on surveillance actors, crowdsourced countersurveillance provides a means of generating ‘hybrid heterotopias’: mediated counter-sites that enable individuals to contest and circumvent surveilled spatial arrangements.

Introduction

For as long as speed cameras and random breath testing have been employed in traffic surveillance, motorists have employed techniques to counteract these surveillance measures. Off the road, individuals have used word-of-mouth to inform their social networks of nearby traffic surveillance measures. On the road, motorists have used ‘headlight flashing’ (briefly switching on a vehicle’s headlights) to warn other motorists of an impending speed trap (see Katz 2000)—a practice that is illegal in many jurisdictions internationally. However, just as traffic surveillance technologies have become more sophisticated, so too have technologies that can be co-opted for countersurveillance.

The advent of networked information communication technologies, including social networking sites, has had a profound impact on countersurveillance praxis. With the rise of social networking sites such as Facebook, new forms of countersurveillance have become possible, enabling users to collectively monitor and circumvent state surveillance measures. Indeed, one of the most prevalent examples of such Internet-facilitated countersurveillance can be found on Facebook, where dedicated regional and national RBT and ‘police presence’ pages publicly post updates on the locations of various forms of police surveillance to subscribers often numbering in the tens of thousands. Whilst the use of such websites for traffic...
surveillance detection and avoidance has been documented by other surveillance studies scholars, including Marx (2016: 149), we wish to provide a more detailed examination of these surveillance neutralization techniques as they pertain to RBT and speed trap pages.

In this article, we argue that Facebook RBT pages exemplify a new form of social media facilitated countersurveillance that we term crowdsourced countersurveillance: the use of knowledge-discovery and management crowdsourcing to facilitate surveillance discovery, avoidance, and countersurveillance. Crowdsourced countersurveillance, we argue, represents a form of countersurveillant assemblage: an ensemble of individuals, technologies, and data flows that, more than the sum of their parts, function together to neutralize surveillance measures. Often, RBT pages, and other crowdsourced police location media such as Waze (2017) and DUIBlock (2017) undertake a form of crowdmapping: crowdsourcing aggregated geographic data to generate digital maps that are updated in real time. Through crowdmapping traffic surveillance, we argue that users may generate what we term ‘hybrid heterotopias’: counter-sites constituted by the online mediation of surveillance and spatial/flow ordering techniques, in which the surveilled spatial arrangement of roads and motorways can be contested and circumvented. Finally, we examine how these traffic surveillance measures are discursively constructed on RBT pages. Through examining the discursive practices of RBT pages, we argue that these domains are as expressive as they are instrumental.

Our article unfolds in six sections. In the first section, we detail the two forms of traffic surveillance targeted by RBT location pages: random breath testing stations and mobile speed-enforcement cameras. In the second section, we review the key literature on surveillance neutralization, linking it to de Certeau’s concept of spatial tactics and Foucauldian conceptions of heterotopia. In the third section, we detail our study’s grounded theory methodology and provide some further detail on the Australian RBT location pages we examined. Though speed camera and RBT location Facebook pages are an international phenomenon, in our research we focused specifically on Australian pages. Our decision to do so was partly out of our familiarity with them and partly to examine the cultural context from which they emerged. In section four, we unpack the concept of crowdsourced countersurveillance and detail its links to existing concepts, including Haggerty and Ericson’s surveillant assemblage, crowdsourced surveillance, and countersurveillance. In section five, we examine the politics of mobility expressed on RBT location pages and argue that such discourses are a symptom of liquid modernity’s valorisation of free-flowing movement. Finally, in section six, we detail how the crowdmapping of surveillance actors through countersurveillant assemblages may generate hybrid heterotopias in public spaces of movement.

**Traffic Surveillance and the Rise of Facebook RBT Pages**

Though traffic surveillance is comprised of an array of fixed and mobile techniques and technologies, the pages we followed primarily targeted two forms of surveillance routinely employed on Australian roads: RBT stations and mobile speed cameras, commonly referred to as speed ‘traps’. Random breath testing is a practice where police located at roadside RBT and mobile drug testing (MDT) stations flag down passing vehicles at random and test drivers’ blood alcohol levels and or the presence of illicit drugs. In jurisdictions where they are utilised, police may require drivers passing an RBT/MDT station to undergo a breath test to determine their blood alcohol level and/or saliva test to test for the presence of illicit drugs (most commonly ecstasy, cannabis, and speed) in the driver’s system. In all Australian jurisdictions, police also have the power to arrest drivers who are over the legal blood alcohol limit (Centre for Road Safety 2014).

Mobile speed cameras are automated speed cameras that are routinely moved to different motorway locations. Often, they are placed in areas determined by speed enforcement officers to have speed-related problems or a high crash risk. In 2017, the Australian state of Victoria deployed over 100 mobile speed cameras, in addition to its close to 300 ‘fixed’ speed cameras situated in permanent locations throughout
the state’s motorways. Victoria Police’s 100 mobile cameras are deployed in 2,000 camera sites, or in 85 stationary and unoccupied ‘camera vehicles’ (Cameras Save Lives 2017).

Though intensified by digital monitoring and tracking systems, technologically assisted traffic surveillance has a long history. Random breath testing was first implemented in Australia in 1976, in the state of Victoria. This was followed by the introduction of RBT programs in the Northern Territory in 1980, South Australia in 1981, New South Wales and the Australian Capital Territory in 1982, Tasmania in 1983, and finally Queensland and Western Australia in 1988 (Homel 1990). Since being implemented in all states, a substantial body of research has evidenced the effectiveness of random breath testing in reducing road fatalities in Australia and abroad (Homel 1988). In all states and territories, the introduction of random breath testing has seen a significant reduction in fatal road accidents. Further, increased levels of RBT enforcement have been found to correspond with reduced state road accident rates (Henstridge et al. 1997; Jiang et al. 2014).

Whilst random breath testing represents a widely accepted and generally uncontroversial form of traffic surveillance in Australia (Watson and Freeman 2007), the same cannot be said of speed enforcement cameras and mobile speed traps. Speed cameras have long polarized motorists in Australia and elsewhere as they are often viewed as a tool for raising revenue, rather than improving road safety (a point we return to in the final section of this article). Like other postmodern surveillance practices (see Staples 2014), speed cameras are automatic, methodical, operate in the local everyday lives of motorists, and monitor wide-ranging populations, rather than just populations perceived to be as suspicious or ‘deviant’.

As noted at the outset of this article, Facebook RBT and speed trap pages represent a new strategy within a long tradition of countermeasures employed against these traffic surveillance measures. However, whilst the aforementioned practice of warning drivers of impending police operations through ‘headlight flashing’ is illegal in several Australian jurisdictions including South Australia (Road Traffic Act 1961 (SA) s.80, Reg.218), communicating the location of overt police operations through social media is not. Nevertheless, police in South Australia and Victoria have expressed frustration at being unable to shut down police presence pages on the social networking site (Kelton 2012). Though they are readily able to identify RBT pages on Facebook through social media monitoring (see Trottier 2015), this represents an ineffective ‘counter-sousveillance’ strategy (see Sandhu 2016) given their lack of legal recourse to demand that the pages be taken offline.

Moreover, Facebook pages are not the only new media platforms dedicated to alerting individuals to the presence of police traffic surveillance. As we will briefly discuss later, smartphone apps with more sophisticated capabilities for rendering traffic surveillance visible en masse are also available, such as DUIBlock (2017) and Melbourne Speed Camera Alert (2017). In addition to offering an avenue for countersurveillance, these smartphone apps and Facebook pages represent surveillance countermeasures: acts undertaken with the aim of frustrating and disrupting surveillance systems (Shay et al. 2013). Moreover, given the illegality of driving under the influence, crowdsourced countersurveillance can also be considered a form of what Goodman (2011) has termed ‘crime-sourcing’: the use of crowdsourcing techniques by distributed networks of criminals to orchestrate and undertake criminalized acts.¹

**Surveillance Neutralization: A Review**

Before elaborating on the new form of countersurveillance RBT location pages represent, in this section we review a number of concepts and phenomena that help further conceptualize our study. This includes the role of spatial tactics in surveillance neutralization and countersurveillance, linkages to Foucault’s

---

¹ Elsewhere, the term crime-sourcing has been used antithetically to refer to criminal investigation by crowdsourcing (Graham 2013).
concept of heterotopias, and analysis of social media as a site of surveillance. As Marx (2016) explains, surveillance neutralization can be undertaken through a range of often-systematically related techniques. These techniques include discovering the location of surveillance actors, avoiding surveillance actors, blocking surveillance actors from functioning as intended, masking one’s identity from surveillance actors, and engaging in countersurveillance: employing the same techniques used by surveillance actors against them (Marx 2016: 145). A number of these moves may be employed to neutralize traffic surveillance. Motorists may avoid locations where an RBT station is located. They may avoid penalty through slowing down for speed cameras. They may also deliberately block mobile speed cameras with their vehicles (Turkus 2015). To confound speed enforcement surveillance, they may mask their identity by employing fake number plates. Finally, upon discovering traffic surveillance technologies, motorists may inform others of their location, enabling other motorists to avoid them in their own travels.

Many of these techniques might readily be read as what de Certeau (1998) terms spatial tactics: opportunistic acts of individual resistance to reclaim freedom and autonomy within the framework of strategies governing a space. Tactics are enacted in response to the institutional strategies of the powerful, and as de Certeau (1998: 7) explains, they depend on ‘clever tricks, knowing how to get away with things, the hunter’s cunning, manoeuvres, polymorphic simulations, [and] joyful discoveries poetic as well as warlike’. Such acts of tactical resistance may, as Hjorth (2005: 392) notes, generate heterotopias: ‘radically other spaces [that] withdraw from the reigning order and the necessities of the present’. A diverse concept originally formulated by Foucault (1970; 1986), heterotopias—literally ‘other spaces’—are spaces that unsettle, counter, or invert normal cultural configurations. For Foucault, the heterotopia ‘puts in place “counter-sites” in which existing social and spatial arrangements are “represented, contested and inverted”’ (Foucault 1986: 24). Though usually conceived as isolated spaces away from the gaze of surveillance and social control strategies (see for example Rymarczuk and Derksen 2014), Allweil and Kallus (2008) extend the term to include ‘public-space heterotopias’: spaces that, despite being located in visible public spaces, have a heterotopian character.

 Whilst we will go on to argue that RBT location pages may similarly be a vehicle for such public-space heterotopias, their collective nature sets them apart from individual surveillance neutralization techniques. Instead, RBT pages represent a collective form of countersurveillance: ‘intentional, tactical uses, or disruptions of surveillance technologies to challenge institutional power asymmetries’ (Monahan 2006: 516). As Marx (2003: 384) proposes, countersurveillance entails ‘turning the tables and surveilling those who are doing the surveillance’. The overwhelming majority of research concerning social media facilitated countersurveillance has related to instances Mann et al. (2003) term sousveillance: the use of wearable or portable image-capture technologies for surveillance purposes (see Goldsmith 2010; Wilson and Serisier 2010; Wall and Linnemann 2014; Brucato 2015). When such portable devices are used to record authority figures or instruments of social control, sousveillance constitutes inverse surveillance.

Surveillance studies have tended to view social media as platforms where institutions can surveil users through automated data collection, storage, and mining (see Fuchs 2011; Werbin 2011; van Dijck 2014; Trottier 2012; 2015), as platforms where users can surveil one another (Trottier 2012), and as platforms for distributing sousveillance footage and citizen journalism (Albrechtslund 2008; Marwick 2012; Trottier 2012). Rarely have surveillance studies scholars examined the affordances social media provide for collectively coordinating and undertaking surveillance or countersurveillance. The closest scholars have come to this issue are recent studies of Internet vigilantism or ‘digilantism’ where social media users, sometimes of their own accord and other times at the behest of law enforcement agencies, collectively attempt to identify perpetrators who have been recorded by other (visual) surveillance technologies (Graham 2013; Nhan et al. 2017). At the heart of this new-media facilitated practice, Trottier (2014) argues, is the phenomenon of crowdsourcing: ‘an online, distributed problem solving and production model that leverages the collective intelligence of online communities to serve specific organizational goals’ (Brabham 2013: xix). In this article, we examine how a very different form of crowdsourcing to
that discussed by Trottier may be employed for countersurveillance purposes—a phenomenon we term crowdsourced countersurveillance.

In examining this new countersurveillance practice, our analysis departs from other research into ‘policing’s new visibility’ (see Goldsmith 2010; Brucato 2015). Its focus is not on ‘cop watching’ (Schaefer and Steinmetz 2014)—that is, visually recording police (mis)conduct and increasing police accountability—but rather on distributing intelligence that enables the avoidance of police surveillance altogether. Much of the research of the former variety has presented as empowering the increased ability to document police conduct via smartphone technologies, and distribute the footage via social media (Yesil 2010; Diamond and Plattner 2012). Though we concur with such analyses on the empowering nature of these technologies, we break from their techno-optimism, and view social media as a tool for conducting both positive and negative forms of countersurveillance. Such forms of ‘citizen journalism’ (see Allan and Thorsen 2009) also differ from the phenomenon we examine here in another crucial sense: their episodic rather than continuous nature. Unlike citizen journalism, crowdsourced countersurveillance is simultaneously continuous and collective; as we will show, it hinges on the cumulative efforts of an entirely voluntary collective.

**Methodology**

We took a qualitative grounded theory approach (Charmaz 2014) to examining the nature and implications of countersurveillance on RBT and speed camera location pages. In employing this qualitatively driven grounded theory methodology, our study focused not on measuring the effects of RBT page countersurveillance, but rather on generating categories for understanding this new form of countersurveillance. Our study did not, therefore, seek to establish the efficacy of RBT pages as a form of surveillance neutralization, nor the frequency of content-categories on these pages. Establishing the efficacy of surveillance neutralization techniques remains methodologically difficult. In examining RBT location pages, our study pursued the more modest goal of developing a conceptual lexicon for understanding this new variant of surveillance neutralization. Like any grounded theory (see Charmaz 2008), our concept of crowdsourced countersurveillance was generated through a process of coding, memo writing, and theoretical sampling. Further, in examining RBT and speed camera pages, we were conscious of not only themes in their textual content, but also their technological affordances (Hutchby 2001), and limitations for engaging in countersurveillance.

Though RBT location pages are an international phenomenon (see DUIBlock 2017), we focus specifically on Australian pages as doing so enabled us to examine the cultural context underpinning page users, anti-speed cameras, and RBT convictions. Between November 2015 and September 2016, we observed 17 Australian RBT and speed camera alert pages on Facebook, and coded posts authored by both the administrators of these pages and their users. The names and details of these 17 pages are tabulated in table 1. There are undoubtedly many other smaller public pages dedicated to smaller regions in Australia, as well as many private ‘closed groups’ which can only be accessed by members. Among the Australian pages we identified, four concentrated on only one form of police surveillance. The remaining thirteen promoted themselves as pages dedicated to revealing the locations of all police operations within an area. Pages dedicated to publishing the locations of portable traffic surveillance are not limited to Australia; in a relatively cursory search we encountered several established within the United Kingdom and the United States. Most (n. 13) of the pages we encountered had over ten thousand subscribers, and three had over 100,000. Of the pages we encountered, the earliest dated back to 2010, with the majority being founded in 2014-2015.
Table 1: List of Australian Speed Camera/RBT Location Pages, August 2016

<table>
<thead>
<tr>
<th>Page name</th>
<th>Region</th>
<th>Likes</th>
<th>Founded</th>
</tr>
</thead>
<tbody>
<tr>
<td>Police in the Area</td>
<td>Australia wide</td>
<td>232,808</td>
<td>23/08/12</td>
</tr>
<tr>
<td>Perth WA Revenue Raisers Alert</td>
<td>Perth</td>
<td>183,221</td>
<td>30/05/11</td>
</tr>
<tr>
<td>Melbourne Revenue Raisers Alert</td>
<td>Melbourne</td>
<td>136,291</td>
<td>31/10/11</td>
</tr>
<tr>
<td>Perth RBT &amp; Booze Bus Locations</td>
<td>Perth</td>
<td>71,767</td>
<td>27/05/13</td>
</tr>
<tr>
<td>QLD Speed Camera Locations</td>
<td>Queensland</td>
<td>64,899</td>
<td>23/05/11</td>
</tr>
<tr>
<td>Block their shot</td>
<td>Australia wide</td>
<td>54,496</td>
<td>1/04/14</td>
</tr>
<tr>
<td>Adelaide Police Locations</td>
<td>Adelaide</td>
<td>50,387</td>
<td>6/9/12</td>
</tr>
<tr>
<td>Victorian Booze and Drug Buses</td>
<td>Victoria</td>
<td>40,596</td>
<td>4/07/10</td>
</tr>
<tr>
<td>Police in the Area</td>
<td>Australia wide</td>
<td>28,038</td>
<td>29/10/12</td>
</tr>
<tr>
<td>WA speed camera locations</td>
<td>WA</td>
<td>26,126</td>
<td>16/05/11</td>
</tr>
<tr>
<td>Police in Werribee and surrounding areas</td>
<td>Werribee</td>
<td>22,274</td>
<td>3/05/13</td>
</tr>
<tr>
<td>RBT/Camera Locations</td>
<td>Canberra</td>
<td>13,021</td>
<td>19/06/11</td>
</tr>
<tr>
<td>Rockhampton and CQ Speed camera locations</td>
<td>Rockhampton</td>
<td>10,830</td>
<td>11/02/13</td>
</tr>
<tr>
<td>NSW RBT Locations Live</td>
<td>NSW</td>
<td>5,264</td>
<td>14/05/14</td>
</tr>
<tr>
<td>RBT Boozebus &amp; Speed Camera Driver Alerts</td>
<td>Victoria</td>
<td>3,736</td>
<td>18/11/13</td>
</tr>
<tr>
<td>Victoria</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RBT and Speed Camera locations in Sydney</td>
<td>Sydney</td>
<td>3,701</td>
<td>22/09/12</td>
</tr>
<tr>
<td>Tassie Speed Camera Alerts</td>
<td>Tasmania</td>
<td>3,005</td>
<td>30/01/13</td>
</tr>
</tbody>
</table>

Our observations, however, came to focus primarily on Melbourne Revenue Raisers Alert and Perth WA Revenue Raisers Alert, two of the most popular pages we encountered. On Facebook, a page’s popularity can be gauged primarily from its ‘like’ count, that is, the number of people who have subscribed to its content using the platform’s ‘like’ button. As of June 22, 2017, Perth WA Revenue Raisers Alert had 183,221 likes, whilst Melbourne Revenue Raisers Alert had 136,291. We ended up focusing primarily on these two pages because they represented not only two of the most popular Australian RBT and speed camera pages, but also two of the most active pages, with their administrators and many users posting numerous updates daily. However, to determine the transferability of the codes and categories developed during the theoretical coding stage of our study, we examined posts on all of these RBT and speed trap location pages. After encountering very similar patterns, codes and practices on each of these pages, we determined that we had reached theoretical saturation and concluded data collection.

Crowdsourcing Countersurveillance

Facebook RBT pages represent a distinct form of countersurveillance that we term crowdsourced countersurveillance: the use of surveillance information obtained from a networked public of crowdsourced labour to engage in the inverse surveillance of law enforcement officials and technologies. The concept of crowdsourcing was first defined by Howe (2006: np), who stated that:

Simply defined, crowdsourcing represents the act of a company or institution taking a function once performed by employees and outsourcing it to an undefined (and generally large) network of people in the form of an open call. This can take the form of peer-production (when the job is performed collaboratively), but it is also often undertaken by sole individuals. The crucial prerequisite is the use of the open call format and the large...
network of potential labourers.

Whilst visual recordings of law enforcement have long been shared with audiences, crowdsourced countersurveillance differs from other forms of sousveillance and countersurveillance in both purpose and practice. Firstly, whereas other forms of countersurveillance are generally undertaken to record police misconduct, crowdsourced countersurveillance is first and foremost a surveillance countermeasure enacted to avoid police detection. Crowdsourced countersurveillance, therefore, combines three of the surveillance neutralization techniques detailed by Marx (2016: 145): discovery, avoidance, and countersurveillance. Secondly, in crowdsourced countersurveillance, images recorded of law enforcement hold a supplementary role to information documenting the location of law enforcement agents. On the pages we examined, in instances where images were posted of traffic police, they served to pinpoint the precise location of traffic surveillance for the purpose of circumvention (see figure 1.1).

![Image](image_url)

**Figure 1.1** Capturing speed cameras: An update on Melbourne Revenue Raisers Alert (2014) pinpointing the location of a mobile speed camera.

Finally, crowdsourced countersurveillance differs from other forms of countersurveillance owing to its collective, centralized nature and, consequently, its scale. Whilst several of the surveillance neutralization techniques detailed by Marx (2016) entail individuals distributing information on law enforcement to large audiences, such information is distributed by individuals working alone. Crowdsourced countersurveillance, by contrast, entails the aggregation of countersurveillance intelligence collected by
numerous actors. Leveraging the crowdsourcing potential of networked media, RBT location pages and traffic surveillance apps centralize and aggregate locational data on public platforms.

For this reason, crowdsourced countersurveillance might—to extend Haggerty and Ericson’s (2000) term—be said to represent an example of a countersurveillant assemblage: an ensemble of individuals, technologies, and data flows that, more than the sum of their parts, function together to neutralize surveillance measures. Indeed, the notion of countersurveillant assemblages provides a particularly productive lens through which to view crowdsourced surveillance neutralization techniques for several reasons. Like surveillant assemblages, countersurveillant assemblages draw together a myriad of technologies. In the case of crowdsourced countersurveillance, smartphones, cars, and social media are assembled into a disparate infrastructure for discovering, mapping, publicizing and avoiding state surveillance measures. Further, like Haggerty and Ericson’s (2000) surveillant assemblage, crowdsourced countersurveillance act primarily as a visualizing device. Through aggregating information provided by a myriad of geographically dispersed actors, crowdsourced countersurveillance generates a fluid real-time ‘data double’ (Poster 1990) of surveillance actors’ locations within an area.

Crowdsourced countersurveillance is, by both definition and necessity, a collective undertaking; its effectiveness rests upon the involvement of a pool of dispersed contributors who, together, can provide a detailed map of police presence within an area. As the surveillance data provided by each contributor are invariably limited, the fewer contributors a page has, the greater the probability of gaps in its intelligence. In addition to a reliance upon a pool of dispersed contributors, a further precondition of this new form of countersurveillance are technologies that enable the collation and communication of contributions. Crowdsourced countersurveillance is, therefore, a distinct product of Web 2.0 and the collection of participatory social media domains that characterise this era of the Internet (O’Reilly 2007). Indeed, it is the possibility of collecting and communicating knowledge to large audiences that separates crowdsourced countersurveillance from previous forms of countersurveillance deployed against social control institutions and agents. Whilst individuals have long used phones and other electronic communications technologies to warn friends of the location of speed traps and police surveillance measures, the ability to disperse this intelligence via such media was limited and typically restricted to one-to-one word-of-mouth communication.

Crowdsourcing, of course, comes in many forms. Notably, the variety of crowdsourcing that lies at the heart of the crowdsourced surveillance discussed by Trottier (2014) differs from the form of crowdsourcing discussed here. Put simply, whereas crowdsourced surveillance primarily involves the collective analysis of data by voluntary labour, crowdsourced countersurveillance involves the collection of data by voluntary labour. Or, to use Brabham’s (2013: 45) typology, crowdsourced surveillance is an example of distributed human-intelligence crowdsourcing, whilst crowdsourced countersurveillance is an example of knowledge-discovery and management crowdsourcing.

As Trottier (2014) notes, surveillance is ordinarily a top-down process undertaken by a small population of specially designated operatives for a similarly small audience. The crowdsourcing of countersurveillance inverts not only the typically top-down nature of surveillance, but also its intended audience. Where surveillance data are typically accumulated for a small but powerful audience of formal social control agents, the crowdsourced countersurveillance of RBT pages is conducted by the crowd and for the crowd. In this way, RBT pages ostensibly resemble the synopticon proposed by Mathieson (1997), where rather than the few watching the many, the many (page subscribers) watch the few (surveillance agents).
The High Road or Highway Robbery? Traffic Surveillance and the Politics of (Auto)Mobility

To obtain crowdsourced intelligence on police activities, RBT and other Facebook countersurveillance pages must mobilise a considerable force of contributors (see Lyon 2005). In this section, we examine the incentives and interests that have mobilised significant participation in RBT pages, through analysing posts on a number of these domains. Resistance to surveillance is often connected to, and driven by, broader social movements, and as Marx (2016), Lyon (2007), and others have emphasized, it is critical that researchers unpack the relationships between these movements and the countermeasures they sanction.

Page users and interested parties need not search far to locate administrators’ views on the surveillance they help circumvent. Administrators regularly stated in posts that their rationale for circumventing traffic surveillance was a scepticism of the expressed purpose of such measures—promoting road safety. For these administrators, traffic, speed cameras, and RBT stations represent not a tool for promoting road safety, but for generating profit (Wells and Wills 2009; Smith and O’Malley 2016). In line with critical stories on speed cameras published by tabloid newspapers (Butt 2013; Smith 2014; Nankervis 2015; Stiles 2015) and motoring enthusiast organisations (see Collett 2015; Maric 2015), speed limit enforcement programs are discursively constructed as tools for revenue-raising (see Delaney et al. 2005; Tay 2010):

this is not the solution to drink driving. the problem is society, psychology and addiction based. some people do not know or will admit they have problem. the penalties are already enough! this is just a revenue raising cash grab!

Melbourne Revenue Raisers Alert (2017)

Flash for cash... Barridale dr Kingsley ..near bridge. How is this anything but revenue raising. I doubt there's ever been a crash in that spot

Perth WA Revenue Raisers Alert (2016)

its time the people challenge the broken revenue raising system to change. its hard for any intelligent person to not apply logic and debunk the propaganda road safety smoke and light show...

Melbourne Revenue Raisers Alert (2016)

Enmeshed within this scepticism of speed limit enforcement programs was a broader distrust of the police. Police officers undertaking speed limit enforcement initiatives were regularly decried by RBT page administrators and users as ‘thieves’ (see figure 1.2), ‘parasites’, and ‘debt collectors’. Anti-police sentiment was pervasive on the two pages we followed, though many users qualified that their enmity towards the police was limited to their involvement in traffic surveillance initiatives (which users often distinguished from ‘real’ police work). Given how pervasive such discourses were on the pages we followed, the crowdsourced countersurveillance of speed traps and RBT stations that occurs through these domains can be read as an act of political resistance. Indeed, one of the foremost anti-covert speed camera organisations in Western Australia goes by the moniker Revenue Raisers Resistance. In the case of Revenue Raisers Resistance, this political resistance goes beyond merely revealing the locations of speed cameras on their Facebook page to include setting up roadside placards alerting drivers of impending police surveillance (Massey and Knowles 2014).
Figure 1.2 ‘Thieves operate in this area’: An update post on Melbourne Revenue Raisers Alert (2016).

Whilst the rationale for circumventing speed cameras was elucidated clearly on most (n. 12) of the RBT and speed trap pages we encountered, the rationale for featuring the locations of RBTs was not. Moreover, given the opprobrium directed at individuals who drive over the legal blood alcohol limit in Australia (exemplified by the TAC’s long-running ‘If you drink, then drive, you’re a bloody idiot’ campaign), their inclusion among the traffic surveillance programs targeted on these pages is more difficult for page administrators to justify. Though the inclusion of RBT pages facilitates avoidance strategies by individuals driving under the influence, several pages feature disclaimers disavowing this criminalized behaviour:

We dont support drink driving. But we do support a stress-free drive. Many people think we shouldnt post Booze Bus locations but why should non drinkers get time taken out of their afternoon by waiting in a line for a booze bus. What if they have a Basketball game they are late for? Or they have kids in the car?


This page is not to help drunk people or criminals, it’s to help our community. If there is a cop comment posted up on where he is, more likely people are going to slow down not speed up if there is a car accident and people post it up you can avoid traffic by using a different route to get somewhere, use this page to help you get around and keep the roads safe for our community.

Police in the Area (2015)

Though these disclaimers might be read as a technique of neutralization (Sykes and Matza 1957) intended to neutralise and disavow the risky behaviours facilitated by these pages, they also reveal the values motivating page administrators. As the disclaimer featured on Perth RBT & Booze Bus Locations indicates, the administrators’ decision to post ‘booze bus’ (RBT station) locations on their page owes to the value they place on unimpeded movement. Whereas speed cameras are represented as illegitimate tools for revenue raising, RBT stations are framed as mechanisms that restrict mobility. Such a concern is not wholly misplaced. At their core, RBT stations and speed traps entail the surveillance of mobility (see Bennett and Regan 2004).
Whilst regularly criticized as tools for profit and revenue raising, like most forms of traffic surveillance, RBT stations and speed cameras are, to use Haggerty and Ericson’s (2000) Deleuzian-based terms, mechanisms for identifying risky flows and removing them from circulation (see also O’Malley 2010; Hunt 2006). Given their relationship to the regulation of flows and mobility, it is useful to situate RBTs within the mobilities studies literature (Urry 2007), and in particular the sub-field of automobilities studies (see Sheller and Urry 2000). Identified as a general principle of modernity (Kesselrin 2006), mobility denotes both actual and potential movements of people, goods, ideas, images, and information (Jensen 2011). Mobility is motive force, velocity, rhythm, route, experience, and friction, however it is more than just these six elements; it is, as Cresswell (2010: 19) remarks, ‘the entanglement of movement, representation and practice’.

Despite an upsurge of interest in mobilities and their intersection with social life over the last two decades, until recently automobility—one of the most dominant forms of mobility—was neglected within the social sciences and related disciplines (Featherstone 2005). Automobility is a combination of autonomy and mobility; however, these combinations produce different experiences and modalities of movement. As Urry (2007: 116) highlighted, the car is interlinked with many different systems, including but not limited to ‘licensing authorities; traffic police; petrol refining and distribution; … car sales and repair workshops’. Further, in documenting the rise of ubiquitous monitoring and tracking systems, (auto)mobilities scholars such as Urry bleakly anticipated that ‘more or less no movement without digital tracing and tracking’ would be possible (289).

Most forms of traffic surveillance are able to pursue their goal of identifying risky flows without disrupting the mobility of motorists. RBT stations, however, are unable to take risky flows out of circulation without slowing the flow of traffic. Given that their proclaimed rationale is to safeguard mobility, the emergence of RBT pages may be read as a symptom of liquid modernity (Bauman 2000), where free-flowing movement is privileged and constant mobility is valorised. As Lyon (in Bauman and Lyon 2013: 6) notes, ‘in liquid modernity power must be free to flow, and barriers, fences, borders and checkpoints are a nuisance to be overcome or circumvented’. Though there is much evidence of their effectiveness in reducing driving under the influence in Australia, on RBT pages, random breath testing stations are viewed as a nuisance—an impediment to a ‘stress free ride’, as Perth RBT & Booze Bus Locations put it. Crowdsourced countersurveillance might, therefore, be read as a tactic (see de Certeau 1998) employed to optimize free-flowing automobility in a liquid modern world.

Whilst RBT pages have an instrumental dimension, RBT pages are also sites of identity and surveillance counter-discourses. In Habermasian terms, posting the location of a speed trap on a RBT page is not just a ‘communicative act’ (Habermas 1984) undertaken by individuals with harmonised plans of action to transmit information and generate understanding. In an era of ‘networked individualism’ (Rainie and Wellman 2012), in which identity is constituted through involvement in multiple dispersed networks, RBT pages provide counterpublics for the affirmation of negative beliefs about state surveillance. Page users regularly echoed administrators’ anti-police sentiment in comments, stating that traffic surveillance represented a form of extortion or revenue raising:

PL: Crimes have gone on the rise because police have chosen to be debt collectors and this is something that they really need to look at.
18 Likes, Melbourne Revenue Raisers Alert (2015)

AP: I dont speed at all, but I am so over these revenue raising cameras, put more Police Patrol Officers on the road, you know, the ones that actually can catch criminals
0 likes, Perth Revenue Raisers Alert (2015)

We are particularly grateful to Caitlin Overington for her insightful thoughts on this subject.
ZK: The police are the tools of financial oppression they work for the financially fascistic government! Any government that needs to fine its citizens $220 for doing walking pace over the ridiculous low limits of 40 50 60km is not a democracy its a hypocrisy!


However, whilst the content of users’ comments indicated that they hold similar attitudes towards the traffic surveillance techniques discussed in this article, their motivations for volunteering information are likely to be varied. We cannot assume that individuals volunteer traffic surveillance locations for the same reason and nor can we assume that individuals who post traffic surveillance locations on these domains routinely contravene road rules.

In addition to investigating the affordances Facebook RBT and speed trap pages provide users for circumventing traffic surveillance, it is also important that we view these domains as sites where attitudes towards surveillance are shaped and reinforced. RBT pages are both instrumental and expressive; through posting the locations of traffic surveillance measures, individuals communicate not only geographical sites of surveillance, but also their attitudes towards these surveillance measures. RBT pages therefore represent key publics for the cultural (re)production of surveillance counter-discourses. They aggregate not only the locations of surveillance actors, but also individuals holding similarly negative views on traffic surveillance.

**Hybrid Heterotopias: Crowdmapping as a Surveillance Neutralization Technique**

Though not all surveillance neutralization techniques hinge on questions of (in)visibility (see Marx 2016), visibility lies at the heart of crowdsourced countersurveillance. In viewing the pre-conditions underlying random breath testing as a social control method, it is clear that the management of visibility is key to maintaining the efficacy of this surveillance measure. As Homel et al. (1997: 3) write, ‘the defining feature of RBT is that any motorist at any time may be required to submit to a preliminary breath test, and there is nothing he or she can do to influence the chances of being tested’. Whilst there are techniques for neutralizing RBT surveillance other than avoidance (see Marx 2016), the efficacy of this surveillance measure is still derived in large part from invisibility.

To use Brighenti’s (2010) term, random breath testing stations operate through a very particular ‘visibility regime’: that is, a systematic, routine, and strategic set of practices that maintain the visibility or invisibility of particular phenomena for particular ends. To function as a general deterrent, random breath testing stations must be heavily mediated, yet geographically invisible. In other words, what must remain visible is the mediated sight of RBTs but not the site of RBTs. As Homel (1988) has argued, the success of random breath testing as a general deterrent is also largely contingent upon the use of extensive publicity. For Homel, the use of televised awareness raising campaigns, such as the Transport Accident Commission’s (2016) ‘The Party’s Over’ campaign in the Australian state of Victoria, are essential to the general deterrent effect of RBT stations and speed traps. Such televised ‘surveillance ceremonies’ (see Staples 2014: 2) remind motorists that their behaviour behind the wheel may at any time be subject to monitoring. However, there is some reason to question Homel’s account of the deterrent value of random breath testing, which broadly accords with a rational choice perspective on offending (see Homel 1993). Few participants in Watson and Freeman’s (2007) study on perceptions and experiences of random breath testing in Queensland Australia, for example, indicated that the risk of police apprehension through this surveillance method had deterred them from drink driving on one or more occasions.

Irrespective of the deterrent efficacy of random breath testing, through publishing their locations in real time, Facebook RBT pages subvert the carefully managed regimes of visibility that optimize this surveillance measure. If, as Homel et al. (1997) posit, the success of RBTs is contingent on the potential
for any driver to be tested at any time, then the proliferation of new media domains dedicated to publishing their locations may further inhibit the effectiveness of this social control mechanism. RBT and speed trap pages, in short, remove the very conditions that underlie the success of these programs. To use Foucault’s (1977: 200) phrase, ‘visibility is a trap’, however, this goes for both speed traps and their targets: the more visible speed traps and RBT stations are in situ, the less effective they become as surveillance tools.

As visualizing devices, countersurveillant assemblages map state surveillance, and in doing so convey spaces and routes where criminalized acts may go unseen by surveillance agents. The RBT location pages we examined used three methods to convey this information. First, they informed their users through short entirely textual posts stating the location of an RBT station or speed camera. Second, several pages collated the crowdsourced information they received into tables detailing the locations of all mobile traffic surveillance within an area on a particular day. Finally, several pages supplemented a number of their textual posts with screen shots taken using Google Maps pinpointing the exact location of RBT stations or speed cameras (see figure 1.3). Through visualizing the locational data they receive from their users, these pages engage in a rudimentary form of crowdmapping. Crowdmapping has been defined by Quaintance (2011) as ‘the aggregation of crowd-generated inputs such as text messages and social media feeds with geographic data to provide real-time, interactive information on events’. Though primarily associated with the mapping of disaster zones—a phenomenon that has been specifically termed ‘crisis mapping’ (Poblet 2013)—crowdmapping has also been utilised to map state crimes (Williams 2013) and elections (Lokot 2015).

**Figure 1.3** Mapping speed cameras: An update on Block their Shot (2014) pinpointing the location of a mobile speed camera using Google maps.

This mapping of speed cameras, RBT stations, and other police surveillance measures differs, of course, from the advanced forms of crowdmapping enabled through software such as the original Crowdmap Application. Facebook’s user-generated fan pages provide limited affordances for undertaking such
crowdmapping. Page administrators must repurpose another site, Google maps, to generate this content, and are unable to collate all the locational data they receive into a single map of an area that can be updated in real time. Recently, applications with more sophisticated crowdmapping capabilities have been developed to fill this void. One such example is Melbourne Speed Camera Alert, a smartphone app—available for download from Google’s app store—that provides real-time updates on the locations of speed and red-light cameras in the city. Co-opting Google Maps, Melbourne Speed Camera Alert’s interface pinpoints on a map of the city the locations of hundreds of speed cameras identified by users.

This crowdmapping and movement of locational data not only creates new pathways through space, but also opens urban spaces of movement in ways that affect everyday life. This can be linked to one of the conditions of late modernity (Giddens 1990)—the transformation of urban spaces into digitized spaces of mediation. Townsend (2000) notes, for instance, that whilst the automobile was the first form of technology that radically altered individuals’ mobility through urban spaces, the advent of mobile Internet connected interfaces such as the smartphone enabled individuals to coordinate themselves and others in real time, across geographically dispersed spaces. The result of such mobile communication technologies opens yet another passageway within everyday urban spaces of movement, adding the circulation of images and information along the virtual-highways of today to the flow of people and objects along freeways, railways, and walkways. In line with this, de Souza e Silva (2006) posits that physical spaces have become ‘hybrid spaces’: mobile spaces that are created by the constant connection of users to mobile interfaces, which are also connected to the Internet and social media platforms. Subsequently, a person can move through urban and online spaces simultaneously, uploading and downloading information as they go about their daily business.

Similarly, through crowdmapping traffic surveillance measures using geographic data, Facebook RBT page users actively construct hybrid spaces that help coordinate new forms of resistance to formal traffic measures. More than just contributing to the hybridised nature of urban spaces of movement, we suggest that RBT pages generate what might be termed ‘hybrid heterotopias’: mediated counter-sites that enable individuals to contest and circumvent surveilled spatial arrangements. Whilst heterotopias are generally conceptualised as discrete and bounded spaces, hybrid heterotopias, we suggest, are not geographically bounded. Rather, they represent a reconfiguration, augmentation, and contestation of everyday spaces through interfacing with technology. In this sense, they are one form of what Stickells (2008: 248) terms a ‘heterotopia of flows’ formed in and through spaces of movement.

Such public space heterotopias are ‘hybrid’ insofar as they are produced by individuals plugging in to online countersurveillant assemblages. To put it in Castells’ (1999) terms, whilst hybrid heterotopias are grounded in ‘spaces of place’, they are constituted by online ‘spaces of flows’: they are simultaneously emplaced and mediated, offline and online. Hybrid heterotopias are entered online but inhabited offline, and they plot a subversive counter-hegemonic cartography over spaces that are otherwise highly ordered. Through connecting to countersurveillant assemblages like RBT location pages, individuals may circumvent surveillance and control measures and transform public spaces of movement into sites and thoroughfares of transgression. RBT location and pages, in other words, may facilitate spatial displacement: altering the location of an intended crime to avoid detection and/or apprehension (Hakim and Rengert 1981). Individuals who regularly drive over the speed limit may slow down to the legal speed limit when passing through a surveilled area, whilst individuals driving under the influence may avoid surveilled areas entirely. If, as Campbell (2013) suggests, crime can be said to reconfigure and choreograph the coordinates of the urban, then the crowdmapping of RBT locations on Facebook represents a subversive remapping of car-only-environments.

In proposing the concept of hybrid heterotopias, it is, nonetheless, important to proceed cautiously and avoid making unsubstantiated claims about the efficacy of RBT pages as a means of circumventing traffic surveillance. As a surveillance countermeasure, RBT pages have several notable shortcomings. To
generate hybrid heterotopias, RBT location pages rely on another form of surveillance: social media surfing (see Albrechtslund 2008). RBT page users must repeatedly monitor their Facebook News Feeds for updates to circumvent sites of traffic surveillance. Moreover, whilst often voluminous, the crowdsourced information on mobile traffic surveillance aggregated on area-specific RBT pages is unlikely to be exhaustive. Consequently, page users still risk detection by speed traps and RBT stations that have not been revealed on these domains.

Further, it is important to note that on Facebook, crowdsourced countersurveillance is mediated by the platform’s algorithmically driven ‘personalisation’ of user’s information environments (see Pariser 2011). As Trottier (2011) notes, Facebook represents a ‘meta-watcher’: all activity by users of the platform is tracked and subsequently employed to personalise their News Feeds. RBT location pages, then, are (counter)surveillant assemblages embedded within a much larger surveillant assemblage. Whilst RBT page users are watching the watchers, Facebook is watching them.

This dataveillance is significant to Facebook-facilitated countersurveillance for several reasons. Firstly, it places the syndication of countersurveillance page posts into users’ News Feeds at the will of an invisible algorithmic curator. Such posts are therefore subject to algorithmic power (Bucher 2012), which influences their visibility within users’ News Feeds and with it, the number of users drawn to such countersurveillance pages. Secondly, it opens RBT pages, and their users, up to the social media monitoring of law enforcement agencies (see Trottier 2015). Finally, it serves as a reminder that such pages remain on the platform at Facebook’s discretion. Facebook is, therefore, far from a digital heterotopia where users can readily contest the practices of institutions away from their gaze. Rather, the platform is a site of hyper-surveillance, where every click and keystroke by users is monitored, and potentially passed on to the very law enforcement agencies RBT pages seek to monitor (see Lynch and Ellickson 2009).

**Conclusion**

With the rise of new and mobile media, the individual tactics of surveillance neutralization described by de Certeau have been supplemented by technologically mediated countersurveillant assemblages. As ensembles of people, technology, and data, countersurveillant assemblages attempt to neutralize surveillance measures through mapping their locations in real time. Plugging in to such countersurveillant assemblages is a subversive spatial tactic—one, which we have shown, that may reconfigure public spaces of movement as ‘hybrid heterotopias’ of risky or transgressive flows. Crowdsourced countersurveillance, we believe, represents just one of many potential configurations countersurveillant assemblages may take.

Distilled to its essence, crowdsourced countersurveillance is characterized by:

1. The crowdsourcing of discovery and countersurveillance neutralization techniques (Marx 2016: 145) to facilitate surveillance avoidance.
2. The aggregation of locational countersurveillance data collected and submitted by a large number of individuals for a (generally) public audience.
3. A technological infrastructure that facilitates knowledge-discovery and management crowdsourcing.

Through offering new affordances for capturing, storing, and distributing information on surveillance actors, mobile and new media have generated unprecedented opportunities for countersurveillance (see Mann and Ferenbok 2013). Crowdmapping the watchers in real time represents just one of many new forms of countersurveillance that have emerged with the advent of social media. As with all countersurveillance strategies, it is also multidimensional and should be viewed through multiple analytical lenses. In examining any form of user-driven surveillance, it remains important to avoid treating
social media as merely a tool or platform employed by users (see Stratton et al. 2017; Wood 2017). Social media should instead be treated as an active mediator of such practices, whose algorithmic architecture, data structures, surveillance practices, and technologically inscribed values shape how such countersurveillance practices unfold and how successful they are.

It is also important that Facebook RBT pages are viewed through both a normative and an analytical lens. Just as we need to consider the ethics, appropriateness, and proportionality of surveillance (see Macnish 2014), so too do we also need to consider the ethics of countersurveillance and surveillance countermeasures. Though its limitations as a harbinger of institutional accountability have been charted (see Brown 2016), sousveillance is often lauded in celebratory terms as a vehicle for empowerment and police accountability. However, like other forms of countersurveillance (see Wilson and Serisier 2010), crowdsourced countersurveillance can generate potentially harmful risk-laden outcomes. Though crowdsourced countersurveillance may be considered a form of empowering surveillance, to use Shilton’s (2010) term, the practices they empower have potentially harmful consequences. For whilst the information aggregated on RBT pages may be used as a legitimate form of political resistance against (arguably) profit-driven speed management programs, it can also be used to engage in risky and criminalised behaviours with a lowered risk of detection and apprehension.

References


Surveillance & Society 16(1)


*Road Traffic Act 1961* (SA), s.80, Reg.218


