Article

Progress in Human Geography
2019, Vol. 43(4) 596–610
© The Author(s) 2018
Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/0309132518772661
journals.sagepub.com/home/phg
SAGE

Resisting geosurveillance: A survey of tactics and strategies for spatial privacy

David Swanlund and Nadine Schuurman

Simon Fraser University, Canada

Abstract

Geosurveillance is continually intensifying, as techniques are developed to siphon ever-increasing amounts of data about individuals. Here we survey three tactics and three strategies for resistance in an attempt to provoke greater discussion about resistance to geosurveillance. Tactics explored include data minimization, obfuscation, and manipulation. Strategies for resisting geosurveillance build upon other forms of resistance and include examination of the assumptions of geosurveillance, investigating privacy-focused software alternatives, and strengthening the ability of activists to operate in this sphere. Individually, each of these are unlikely to effect great change; used in concert, they have the potential to guide technological development in such a way that it is less likely to serve corporate and government interests and more likely to protect individual and group privacy.

Keywords

biometrics, geosurveillance, resistance, strategies, tactics

I Introduction

On 5 April 2017, Canada's RCMP admitted to using International Mobile Subscriber Identity (IMSI) catchers, commonly known as Stingrays, to conduct surveillance of Canadians' cell phones (Seglins et al., 2017). IMSI-catchers act as a cellular base station, tricking nearby phones into connecting to it rather than their usual provider's stations. This allows the device to log which phones are nearby and can potentially also siphon up text messages and intercept phone calls. While the RCMP assured the public that IMSI-catchers were only used during emergency scenarios, and that no phone calls or text messages were intercepted, the discussion surrounding their use in the US has been raging for years. In 2015 it was revealed that the FBI had been mounting IMSI-catchers to planes and flying them over US cities (*The Guardian*, 2015), conduct that was mirrored in Anaheim by local police (Zetter, 2016).

One of the contentious aspects of IMSI-catchers is that, by design, they collect data on every phone that surrounds them; they collect the entire haystack to find a single needle. Moreover, there is evidence they have been used at protests, essentially to collect the entire haystack in case needles emerge at a future date

Corresponding author:
Nadine Schuurman, Department of Geography, Simon Fraser University, 8888 University Drive, Burnaby, BC, V5A 1S6 Canada.
Email: nadine@sfu.ca

(Rivero, 2015). It is because of these facts that recent media has been critical of IMSI-catchers (Biddle, 2016; Snowdon, 2016; Zetter, 2015), and that organizations such as the American Civil Liberties Union are launching Freedom of Information Act (FOIA) requests and lawsuits to uncover and mitigate their use (American Civil Liberties Union, 2015; K. Martin, 2016).

IMSI-catchers are quintessential mechanisms of *geo*surveillance, that is to say surveillance that incorporates or focuses on spatial location. They are used by the state to secretly trawl large geographic spaces and capture the location of every cell phone within those spaces, typifying the 'whole-haystack' approach to surveillance. At the same time, they are increasingly becoming entangled with resistance. One aspect of this entanglement is that their alleged use to limit resistance at protests has inspired direct and significant resistance to them. Another aspect is that they, like many other technologies, represent something that is superficially trivial and yet proves effectively hopeless for the average citizen to resist. It is trivially easy to either not own or turn off a mobile phone, but social organization make this incredibly difficult to do in practical terms, and this difficulty is likely to only increase with time.

Geosurveillance mechanisms such as cell phones can, at least, be turned off. Other mechanisms are being constructed that allow no such recourse by individuals. Biometric technologies, including facial recognition (Hill, 2015), gait analysis (Ioannidis et al., 2012), and wireless heartbeat sensors (Conner-Simons, 2016), are being developed with immense potential to track bodies moving about spaces, as unlike cell phones or social media, they do not require citizens to 'opt in'.

Intrusions on our geoprivacy are particularly concerning due to the highly revealing nature of spatial data. Leszczynski (2015) succinctly identifies four specific concerns for geoprivacy with regard to spatial data:

> i) spatio-temporal location is seen to constitute definitive proof or evidence of individuals' involvement in specific behaviours, activities, and events in space, or as proof of the potential of their involvement; ii) the extensive, exhaustive, and continuous nature of geosurveillance (Kitchin 2015) means that there is no feasible way of achieving or maintaining spatial anonymity within data flows; iii) spatial-relational data is inherently meaningful beyond being locational, revealing other intimate aspects of our personal lives; and iv) unlike other forms of PII, spatial data carries with it information that can be used to translate threats to our personal safety and security into actual harms to our person. (2015: 9)

As such, we focus this article on ways and means of resisting geosurveillance, both in the short and long term. We seek to explore techniques for resisting the potential negative privacy impacts that geosurveillance carry. That is not to say that we attempt to provide an exhaustive set of techniques for resistance, but rather to merely provoke more engagement with potential tools, both technical and theoretical, for resisting geosurveillance.

In doing so we offer a straightforward implementation of Michel de Certeau's (2011) framework that differentiates methods of resistance between tactics and strategies. This framework was chosen based on a review of the resistance literatures and on conceptual grounds. Most notably, we were drawn to its ability to integrate a wide range of other theoretical tools, as well as its ability to put those theoretical tools to work in practical applications. Indeed, we hold that critical GIS should engage both theory and practice, and a framework of tactics and strategies allows us to handle both simultaneously.

For Certeau, tactics are employed at opportune moments or when power cannot be pinpointed, while strategies locate a specific power and coordinate resistance against it (Certeau, 2011). As such, we refer to tactics as the immediate, short-term techniques for evading, challenging, frustrating, or otherwise temporarily disrupting the operation of geosurveillance. We refer to strategies, on the other hand, as the long-term, large-scale struggle against the power that enacts geosurveillance. For example, tactics for resisting surveillance may include using encrypted messaging, but a long-term strategy may be to effect stronger legal protections such that evasion is no longer necessary.

Of course, tactics and strategies for resistance must be tailored to surveillants. In this article, however, we present generalized tactics and strategies that might be used against any type of data collection, but contextualize them with specific and purposefully familiar spatial examples for clarity, such as the sale of spatial social media data. Nevertheless, it must be made clear that surveillance is conducted by a wide variety of parties for myriad purposes through countless mechanisms (Kitchin, 2015; Swanlund and Schuurman, 2016). Examples of these might include the National Security Agency conducting surveillance for security purposes by watching internet traffic, Facebook collecting location data for market research and advertising through browser APIs, law enforcement monitoring cell phone locations for policing through IMSI-catchers, or even municipal governments tracking daily commutes through transit passes. Importantly, different tactics and strategies for resistance should be used for each of these cases, and our examples are by no means exhaustive.

The first section of this article will begin with a literature review, surveying scholarship on geosurveillance and resistance to surveillance both within and outside of the geographic literature. The second section will explore tactics for resisting geosurveillance and their attendant limitations, while the third section will explore strategies for resisting geosurveillance. Finally, we conclude by discussing limitations and potential future research.

II Literature review

A substantial body of literature exists within geography on geosurveillance and geoprivacy. As far back as the 1990s geosurveillance was a hotly contested topic due to the rise of geodemographics (Curry, 1997; Goss, 1995). Since then, data collected about us has become significantly more abundant, granular, and personalized, resulting in continued engagement among geographers with the privacy implications of spatial data. These engagements have approached geosurveillance and geoprivacy in a variety of ways. For instance, scholars have looked at how the smart city movement has resulted in exhaustive geosurveillance (Kitchin, 2015), the way that new spatial media can have highly gendered implications for geoprivacy (Leszczynski and Elwood, 2015), the problems inherent to geodemographics and their continued relevance to spatial big data (Dalton and Thatcher, 2015), and the ways that spatial big data complicate geoprivacy as is revealed by government surveillance (J. Crampton, 2014), among many other topics (Armstrong and Ruggles, 2005; J. W. Crampton, 2007; Elwood and Leszczynski, 2011; Leszczynski, 2015; Murakami Wood, 2017; Swanlund and Schuurman, 2016).

Unfortunately, the notion of resisting geosurveillance has yet to be directly explored. Obviously, resistance is not foreign to geographers, and has been contemplated abundantly in a variety of forms. These include, for example, examinations of resistance in the context of neoliberalism and globalization (Bakker, 2013; Featherstone, 2003; Sparke, 2008), as well as autonomy and autonomous geographies (Naylor, 2017; Pickerill and Chatterton, 2006). When the topic of resistance does arise in the context of geosurveillance, it often functions as a token of hope after a long and dismal explication of our grim present (Goss, 1995; Swanlund & Schuurman, 2016). Although there is a rich body of research on resistance and surveillance, the notion of resisting geosurveillance specifically has received less scholarly attention. Closest to this is Amoore and Hall's (2010) exploration of how artistic expressions can effect a resistance to border security. While the article is deeply informative, geosurveillance remains tangential to it.

Within the broader discipline of surveillance studies, resistance is a theme that has been characterized as 'underdeveloped' (A. K. Martin et al., 2009). Nevertheless, what work has been done has been valuable. The most notable theme that has emerged throughout the literature concerns the capacity of resistance to surveillance. Some scholars have been cynical of the ability for the average citizen to enact meaningful resistance, either because they lack the legal, technical, market, and political affordances to do so (Calo, 2016), or because resistance often results in an arms race between those who conduct surveillance and those who resist it (Leistert, 2012).

This capacity for resistance has also been critiqued on an organizational level (Dencik et al., 2016; Introna and Gibbons, 2009). There is a noted disconnect between those activists who resist surveillance, and those that are subject to it (Dencik et al., 2016). This disconnect extends to online advocacy organizations, such as the Electronic Frontier Foundation (EFF), whose lack of coordination and cohesiveness between themselves and others, as well as the constraints of only operating in the US, limit their ability to effect change (Introna and Gibbons, 2009).

Nevertheless, others have provided more optimistic accounts of resistance. Gates (2010) recounts the introduction of facial recognition into a community in Tampa, and the resulting backlash against the effective increase in police power that successfully halted the program. Sanchez (2009) provides a similar story, wherein changes in Facebook's timeline resulted in immense online protest against the social networking website due to its consequences for privacy, leading to subsequent changes. Finally, Mann and Ferenbok discuss the rapid development of technology as being conducive to the rise of sousveillance (when those with less power watch those in power), which they believe could 'challenge and balance the hypocrisy and corruption that is otherwise inherent in a surveillance-only society' (Mann and Ferenbok, 2013: 18). These examples should serve as a reminder of the incompleteness of power. Indeed, as Pickett (1996) writes, 'power may form disciplined individuals, who are rational, responsible, productive subjects, yet that is in no way an expression of a human' (p. 458).

Returning briefly to the geographical literature, while geographers' addition of 'geo' to 'surveillance' implicitly signals that space plays an important role in how forms of surveillance operate as well as the data that are collected, there has been less attention to how the uniqueness of spatial characteristics might affect methods of resistance. It should be of no surprise, for example, that it is much easier to resist the surveillance of text messages (there exist a grab bag of apps that do this) than it is to resist the surveillance of where those messages are sent from (a fundamentally hard technical problem). This is true even politically: whereas the content of our conversations typically merits strong legal protection, spatial data often slips through the cracks of legal protection due to it being considered meta-data, reducing the surface of legal challenge (Privacy International, n.d.). It is for this basic reason that although surveillance studies scholars may perform critical work regarding resistance (Calo, 2016; Dencik et al., 2016; Mann and Ferenbok, 2013), this work may not fully substitute for the kind of spatial perspective that a geographer might contribute.

III Tactics for resisting geosurveillance

Tactics are the short-term, immediate techniques for evading, challenging, frustrating, or otherwise temporarily disrupting the operation of geosurveillance. We provide three categories of tactics that can be used to resist geosurveillance, including minimization, obfuscation, and manipulation. Within each category, we briefly describe relevant tools and techniques, as well as the advantages and disadvantages of each type of tactic. It should be noted that this list is far from exhaustive. In fact, it only includes tactics that affect data collection, and does not include such forms as artistic expression, civil disobedience, or public protest.

Moreover, some of the tactics described may not always clearly resemble acts of resistance. For instance, consider a VPN user that has no strong opinions on issues of privacy and surveillance, but merely uses a VPN to either hide their location when torrenting movies, or to receive content that is geographically locked by streaming services, such as from Netflix or Hulu. This use-case is common, and users may hardly consider it to be an act of resistance. Nevertheless, it may function as such.

To illustrate this, we look to James Scott's notion of everyday resistance, wherein even small acts of resistance are still seen as meaningful, despite their lack of revolutionary potential (Scott, 1987). Accordingly, Campbell and Heyman's (2007) notion of slantwise action is useful here, which expands on Scott's work. The authors describe instances wherein 'people frustrate the normal play of a given power relation by acting in ways that make sense in their own frameworks but are disconnected or oblivious to that power relationship's construction or assumptions' (2007: 4). These represent slantwise actions, or actions wherein individuals may have no outright motive of challenging power structures, but their actions do so regardless. Indeed, slantwise actions enable us to imagine actions that fall in between the tidy dichotomy of power and resistance. Referring to the example of self-interested VPN users, we consider their use of VPNs to be an example of slantwise action. While they may have no explicit motive to challenge the powers that conduct geosurveillance, their actions nevertheless can frustrate them. We continue with the assumption that this type of action is valuable, and encourage others examining resistance not to ignore it.

1 Minimization

The simplest tactic to resist geosurveillance is surely to minimize opportunities for data collection. While there are a multitude of mechanisms for enacting geosurveillance that make complete avoidance impossible (Swanlund and Schuurman, 2016), reducing the number of data points about one's self remains an effective act of resistance. It is effective because, although surveillants may be able to separate the signal from the noise in obfuscated or manipulated data, reducing the amount of signal in the first place is likely to work.

Minimization may take many forms. An overlooked aspect of geosurveillance, however, is the spatial data we create when we conduct payments. Every purchase made at a store with a credit or debit card is associated with that store, meaning that our purchases leave trails of where we go. A simple minimization tactic is to instead pay with cash, which is effectively anonymous. Alternatively, Bitcoin provides us with the possibility to do this electronically, both in the physical world as well as the digital, although this has yet to achieve any mainstream adoption.

On the other hand, minimizing spatial data trails involves not using technologies that are increasingly embedded into social life. Paying with cash comes at the cost of building a credit score, which could affect one's ability to acquire a mortgage later in life. Thus, removing such technologies from daily life often comes at the cost of social agency, a trade-off many are not willing to make. Additionally, minimization itself may arouse suspicion now that having an extensive data double is the norm. When minimization is not an option, obfuscation or manipulation may be the solution.

2 Obfuscation

Obfuscation has been a particularly popular tactic for resisting surveillance. Websites such as Internet Noise load random pages to confuse and obfuscate one's digital trail (Schultz, n.d.). The goal is to add noise to the myriad of profiles generated about us. Internet Noise, for example, does this to obfuscate our interests from corporations that purchase our internet histories from internet service providers. As the author of the tool describes, it 'will start passively loading random sites in browser tabs. Leave it running to fill their databases with noise'. While this method of obfuscation has drawn some criticism (Waddell, 2017), it remains popular, with several independent implementations (Howe & Nissenbaum, n.d.; Schultz, n.d.; Smith, 2017).

The notion of obfuscation as resistance has been thoroughly explored by Brunton and Nissenbaum (2015), who liken it to camouflage, and suggest it is 'suited to situations in which we can't easily escape observation but we must move and act' (p. 50). Regarding geosurveillance in particular, one of the most popular methods of obfuscation is the Tor network. The Tor network routes traffic through a series of three servers that, combined with the use of cryptography, provides strong anonymity, particularly spatial anonymity. Another example of spatial obfuscation that Brunton and Nissenbaum (2015) provide is CacheCloak, a system for location-based services that hides your actual route by also predicting and retrieving many other permutations of it. The result is that any surveillants wouldn't know which of the retrieved routes was the actual one taken.

Of course, spatial obfuscation only works in a limited number of ways. For example, obfuscating one's location from their cellular provider and credit-card company would require them to frequently and randomly shuffle phones and cards between a large group of people. While few would ever consider taking these measures, if they did they would have no guarantee of success. In fact, analysis of 'anonymized' credit card data found that it only took four transactions to identify 90 per cent of individuals (Montjoye et al., 2015). In this way, spatial obfuscation may be significantly harder than obfuscation of other types.

3 Manipulation

Whereas obfuscation involves adding random noise to make patterns harder to recognize, manipulation involves adding specific noise to craft specific patterns. Crawford (2016) highlights ways that algorithms can be manipulated or gamed when she describes how members of 4chan and Anonymous used their knowledge of voting algorithms to spoil the results of a Time.com poll. This reveals the potential for individuals to use their knowledge of how surveillance operates to manipulate their data trails to their advantage. Manipulating spatial data in particular can be incredibly powerful, in part because of the aura of 'truth' that is often ascribed to where we are (Leszczynski, 2015). Thus, if we can forge this 'truth' in a way that is advantageous to us, we can transform the negative impacts of geosurveillance into positive ones.

The aforementioned example of using a VPN to bypass geographic content restrictions, such as those enforced by Hulu, Netflix, and YouTube, constitutes one manipulation of spatial data. To provide another example, an individual concerned about the insurance industry purchasing data about them to gauge their health might use Facebook's check-in feature to check into health food stores, gyms, and yoga studios as they walk past them to an adjacent fast-food restaurant. This could be extended to tools that function similarly to Internet Noise, which, rather than making random Google searches, could make Google searches specifically associated with healthy living, such as 'nearest

Whole Foods', 'local running clubs', and 'Vancouver cycling stores'.

Manipulation makes obvious the naivete of the assumption that spatial data can be a reliable indicator of who we are. Obviously, the disadvantages of manipulation are similar to those of obfuscation, namely the added input required to craft false signals, as well as the fact that it cannot easily be extended to all types of data collection.

Used together, these tactics can not only protect individuals from various forms of geosurveillance, but can turn it to their advantage. While we only presented three potential categories of tactics along with a handful of examples, we encourage others to contribute to the conversation. For instance, in 2003 Gary Marx developed a strong taxonomy of 11 intuitive 'moves' for resisting or neutralizing surveillance, such as avoidance, masking, refusal, and counter-surveillance moves. While Marx's moves were largely aspatial, they may be adapted to geosurveillance specifically, and could prove fertile ground for future research. Of course, these tactics on their own are unlikely to prompt larger-scale reform that mitigates geosurveillance. For this, longer-term strategies are required.

IV Strategies for resisting geosurveillance

We present three meta strategies for resisting geosurveillance. These include: destabilizing the core assumptions of geosurveillance, building secure and privacy-friendly alternatives to common software applications, and fostering stronger activism against geosurveillance.

1 Destabilizing core assumptions

The core assumptions behind geosurveillance are often inherently fragile, and unpacking them quickly reveals their weaknesses. For instance, two core assumptions that frequently underlie geosurveillance are that (1) data about us is always an accurate representation of ourselves, and that (2) this data can be used to calculate our future actions. The first assumption has been challenged by artist Hasan Elahi, who performed extensive self-surveillance, but did so in a way that allowed him to carefully construct a narrative about his life (Kafer, 2016). In other words, Elahi used the tactic of manipulation (wherein data is specifically crafted to produce an advantageous false narrative) to demonstrate how data about ourselves is malleable and subject to interpretation. The second core assumption has also already been challenged by Louise Amoore (2014), who shows that for the modern security state 'calculability is never in question, [as] a precise arrangement of combinatorial possibilities can always be arrived at in advance' (p. 435). In this way, the security state assumes that given the necessary data, anything and everything can be calculated, and nothing can escape mathematical prediction or explanation. These constitute valuable works that destabilize the core assumptions that geosurveillance often rests upon.

Nevertheless, there is still much potential for future work. For instance, a third assumption that facilitates geosurveillance lies in the interpretation of the word 'metadata'. Experts have noted that where people travel, who they talk to, and at what times these occur used to be the information one would hire a private investigator to gather, as each can reveal a significant amount about an individual's life (Schneier, 2014). Today, however, these revealing details are relegated to the status of being 'just metadata'. It is this devaluation that has enabled intelligence agencies and corporations to siphon up spatio-temporal data and squirm around legal protections that would otherwise protect privacy. Therefore, we believe a genealogy that explores this fundamental shift in values that modern geosurveillance is dependent upon would be a strong starting point for resistance.

Finally, Dencik and Cable (2017) highlight a phenomenon that they call 'surveillance realism'. Surveillance realism is a perspective of resignation that many in the public hold that stems from the 'lack of transparency, knowledge, and control over what happens to personal data online' (p. 763). We see the destabilization of core assumptions as a potential countermeasure to surveillance realism. What is necessary for this work to be effective, however, is strong communication with the public. Indeed, it is crucial that these challenges to the core assumptions of geosurveillance do not remain in the depths of libraries and archives. Knowledge translation in this context is as important as the knowledge itself, or else the public will continue to resign themselves to the apparent inevitability of geosurveillance.

2 Building private alternatives

The second potential strategy is guided by the work of Donna Haraway's essay, 'A Cyborg Manifesto' (1991), where she identifies the creation of the cyborg, a hybrid constructed by the increasing integration of technology into the human experience. The cyborg has been, and continues to be, a fruitful figuration for geographers (Kitchin, 1998; Schuurman, 2002, 2004; Wilson, 2009). Notably, however, Haraway remarks that the cyborg has yet to be fully written (Haraway, 1991). It is this gap, she argues, that allows women to actively write the cyborg themselves and define its forms, rather than to watch its development from afar and be subject to the consequences of its masculinist origins (Schuurman, 2002). In other words, it represented an opportunity for women to '[seize] the tools to mark the world that marked them as other' (Haraway, 1991: 171).

It is in the same vein that resisting geosurveillance should not be at odds with technological progress. As others have argued, outlooks towards technological progress often fall into the binary of extreme optimism or dire pessimism (Kingsbury & Jones III, 2009). However, technology can develop in either direction simultaneously, and there is no shortage of middle-ground. These two theoretical perspectives grant us significant agency insofar as they allow us to seize the opportunity to write our own futures, and to guide technological progress as we see fit. In this way, we view the construction of technologies that offer alternatives to be of great importance to the broader goal of resistance.

The development of CacheCloak is a spatial example of this. A more popular example amongst technologists and developers, on the other hand, is Piwik. Although it is not targeted towards end-users, Piwik may affect them regardless, whether they know it or not. Indeed, while Google's Analytics reigns supreme on the web, the result of that dominance is that users can be tracked by Google across many different websites. Piwik, on the other hand, is an open source project that offers locally hosted analytics with far stronger privacy features (Piwik, 2017). Significantly, it is easily configured to anonymize IP addresses (locations), offers easily-embeddable forms that allow users to opt out of its tracking, encourages website administrators to only keep data in aggregate after a certain time period, and allows websites to gain useful analytics about their users without necessarily forfeiting that information to third parties as well (such as Google). Importantly, it can be used by small and large websites alike, meaning it provides an alternative not just for individuals, but for large corporations that interact with millions of users daily. And, as a result, Piwik has achieved considerable success, with deployments by T-Mobile, Wikimedia, Forbes, Sharp, and Oxfam, among many others (Piwik, 2017). Due to its capabilities, design, and achievements, we believe that Piwik represents an ideal model for building alternative software that respects privacy without sacrificing functionality, and without rejecting technological progress or denying the needs of website operators to collect basic analytics.

Piwik, however, is not the only successful software alternative that provides stronger privacy than conventional software. Signal offers private instant messaging, Bitcoin offers more private online payments, OwnCloud offers private cloud storage, and Protonmail offers private email. Each of these examples utilize cryptography and open-source design such that users can verify for themselves that their privacy is protected. While this is admittedly difficult for all but the most technical users, the fact that code can be audited at all by the public makes covert privacy intrusions far riskier to implement, and encryption denies the surveillance of content regardless of how much these projects scale. What is lacking, however, are software alternatives for location-based services with strong privacy built-in. While CacheCloak is inventive, an application has yet to be released. OpenStreetMap is often celebrated for being open source, but it features no technological affordances to protect user privacy (such as encryption), only policies. Private location-based services are severely lacking, and represent a significant area that needs new tools and alternatives.

Unfortunately, alternatives cannot be easily constructed for everything. For example, fundamental challenges exist for protecting the geoprivacy of our mobile phones. IMSI-catchers exploit the architecture itself of cellular networks, meaning that building in privacy protections would require either overhauling the way mobile phones operate across the board, or enacting stronger legislation.

3 Strengthening activism

Finally, stronger activism from a wider variety of participants will extend the reach of the first two strategies, and will itself bring privacy closer into reach. Of course, activism may seem an obvious and simplistic candidate. In fact, analysis of US politics has shown that public opinion has no significant impact on political decisions (Gilens and Page, 2014), making activism seem like a lost cause. Calo (2016) reinforces this sentiment, citing the power of special interests in the intelligence community and the historical success of surveillance over privacy. However, activism is integral to resisting geosurveillance as it remains the only concrete and direct way to challenge that which cannot easily be resisted tactically, such as mobile phone surveillance or facial recognition. And sometimes, albeit rarely, it works (Gates, 2010; Sanchez, 2009).

For activists, strengthening activism means forging greater external connections. Unfortunately, anti-surveillance activism falls to a small group of technologically knowledgeable individuals and organizations (Dencik et al., 2016). The implication of this is that those who advocate against surveillance are often not the ones affected by it. Rather, those who are affected by surveillance advocate for other causes, such as environmentalism or animal rights. This mismatch limits the potency of anti-surveillance activism. Therefore, the adoption of a data justice framework may aid in achieving greater anti-surveillance activism from those who usually advocate for other issues. As Dencik et al. (2016) explain:

> By advancing the framework of ‘data justice’ our point is to illustrate how the relationship between political activism and surveillance is not one in which activists are only at risk for expressing dissent, but one in which the very infrastructures of surveillance (dataveillance) have direct consequences for the social justice claims they are seeking to make. That is, we can use this notion to argue that concerns with the collection, use and analysis of data need to be integrated into activists’ agendas, not just to protect themselves, but also to achieve the social change they want to make. (2016: 9)

Therefore, data justice unites a wider range of activists around the ways that data, including its collection, use, and representation, are fundamentally intertwined with their causes. Fortunately, the notion of data security is already being raised in the public consciousness as security training sessions, known often as Cryptoparties, become more popular, particularly for activists (Kalish, 2017). Explicitly inserting elements of the data justice framework into these workshops may be a worthwhile vector for ensuring its meaningful adoption among activists.

For academics, on the other hand, strengthening activism means, among other things, aiding the ability for activists to do work and have voice. While it need not be limited to only academics, Lubbers' (2015) proposed research domain of 'activist intelligence and covert strategy' calls on academics to shed light on how activists are covertly spied upon by corporations and the police, and how corporations control debates and silence dissenting opinions. Such research could often take on an investigatory style to uncover activist surveillance, but could also include contextualizing the social, political, and technological conditions that enable and provoke it. Lubbers (2015) identified that the ability for activists to have and exercise voice, particularly dissenting voice, is regularly undermined. In this way, research into activist intelligence and covert strategy both functions as and aids resistance. Once again, however, it is paramount that such research is properly translated to the public so that can effect as much change as possible.

V Discussion

If, as Foucault asserted, power produces not only subjects but opportunities to resist it (Foucault, 1995), then minimization, obfuscation, and especially manipulation are surely the opportunities of resistance that are directly enabled by the exercise of geosurveillance. Indeed, the possibility of obfuscation and manipulation is reliant upon the collection and operationalization of data about the individual who obfuscates or manipulates. In fact, in some cases increased data collection actually benefits the individual who uses these tactics. As Kafer (2016) notes, extensive self-surveillance has enabled artist Hasan Elahi to manipulate a narrative of his life that, on the one hand, seems detailed and true, but, on the other hand, leaves just enough pockets and gaps for him to achieve a certain degree of agency. Kafer notes that 'because Elahi's GPS coordinates and cell phone photography are only periodically updated, these intermittent updates allow for slippages in the complete disclosure of his activities, such that he could, for example, easily make trips to a storage unit in Florida if he had the chance' (p. 236). In short, although we are being constantly shaped as subjects through various forms of surveillance, all hope is not lost, but rather this subjection produces new opportunities and possibilities for our own resistance (Foucault, 1995).

However, these molds that shape our subjection are in continual flux. Just as Deleuze (1992) suggested that we now live in societies of control that function 'like a self-deforming cast that will continuously change from one moment to the other' (1992: 4), geosurveillance is adapting to a new moment that disintermediates its operation, enabling it to work more closely on the individual body and its constituent parts. Biometric technologies such as facial recognition can identify individuals and record their presence at a location, without subjects consenting even implicitly (such as by carrying a cell phone). Moreover, second generation biometrics enable surveillants to collect data wirelessly about the body and subsequently infer our emotions and intents, also enabling the tracking of emotions across spaces (Mordini et al., 2012; US Department of Homeland Security, 2014). Therefore, whereas the mechanisms of geosurveillance discussed throughout this article would be operationalized by building a history or narrative about someone, biometrics can now calculate our emotional status or intent in real time across space, ‘like a self-deforming cast that will continuously change from one moment to the other’ (1992: 4). This, of course, has significant implications for resistance.

For instance, obfuscating or manipulating biometric data, particularly variables such as heart-rate and micro-scale vocal fluctuations, is unrealistic, if not impossible. While minimization may technically work, due to their advancing wireless capabilities one might not always be aware of when biometrics are being used. As such, biometrics significantly reduce the surface for the methods of tactical resistance presented here, meaning resistance to biometric geosurveillance may require new tactics as well as stronger strategies. This is not to suggest that biometrics will replace the current methods of geosurveillance, but rather that they will likely supplement them. Therefore, the tactics we outline here will remain relevant to many extant forms of geosurveillance, while the strategies will become far more integral to effecting meaningful resistance. Nevertheless, far more theorization of resistance to geosurveillance is warranted given the capabilities of these new technologies.

While not explicitly a re-theorization of resistance, our taxonomy of tactics and strategies points in the direction that we believe such a re-theorization should take. In essence, tactics and strategies are mutually reinforcing elements that are both integral to resistance. Tactics provide real, tangible outlets for resistance that can be enacted immediately or encouraged in a slantwise fashion against a given instance of surveillance. Strategies provide long-term methods and goals towards a broader challenge of the power structures that enact surveillance. They are more powerful together than they are singularly. Meaningful real-world resistance cannot be a theoretical construct in nature or an academic maxim. Likewise, resistance cannot be entirely composed of slantwise tactics; there must be some identification of the broader power structures at play, and theorization of how they can be deconstructed. Strategies should inform tactics and tactics should engage strategies. And both require theoretical scaffolding as well as real-world coding.

VI Conclusion

This article offers several tactics and strategies for resisting geosurveillance. Tactics include data minimization, obfuscation, and manipulation, while strategies include destabilizing the core assumptions of geosurveillance, building privacy-focused software alternatives, and strengthening activism and the ability for activists to operate. The article’s contribution is therefore in its aggregation and contextualization of these methods, as well as its provocation for further discussion and research, particularly considering the recent advancements of biometric technologies. Of course, no single tactic or strategy will bring about meaningful change, but when used in careful concert with one another they have the potential to shift technological development to less dominating results.

As its final and potentially most significant contribution, this article renews one of its authors’ assertions about critical GIS made nearly two decades ago in this very journal: that critics must do more than just critique (Schuurman, 2000). They must engage with the technology at which their critiques are aimed, communicate using its vocabulary, and deliver their critiques constructively and in ways that can be readily operationalized by its users. In writing this article we have attempted to follow this prescription.

Nevertheless, while these methods have the potential to effect significant resistance, they are not without limitations. First, we survey only a handful of broad solutions. Many more clearly exist, and we encourage others to examine how they might be applied to geosurveillance, as well as to unpack their intricacies. Additionally, research into how slantwise resistance might be engineered, as well as the ethics of doing so, would be valuable. Such research would ask what incentives could be built into acts of resistance, such that self-interest alone could motivate individuals to act, as well as whether such engineered politics are at all ethical.

Second, the methods for resistance that we have described are all highly contingent. Individuals operating in heavily surveilled and censored countries, for instance, may have little strategic agency, and certain tactics may not only be unavailable but have significantly higher stakes if used unsuccessfully. Moreover, they all rely on extensive knowledge of how geosurveillance operates. Knowing how to manipulate location data requires an understanding of how that data might be collected and repurposed. Even slantwise tactics, such as using a VPN to evade content restrictions, require some technical ability that many do not possess. While this barrier may be reduced as younger generations familiar with technology grow older, it must also be acknowledged that technology may simultaneously get more advanced and 'black-boxed'. Therefore, social agency, technical literacy, and transparency may be impediments, and future research should seek to address them.

Third, tactics that have been presented are based entirely on controlling data flows. Unfortunately, biometric technologies are emerging that remove this control and operate from afar. Facial recognition, gait recognition, and even mood sensing are rapidly developing technologies that are increasingly being deployed in the real world (AutoEmotive, n.d.; Hill, 2015; Ioannidis et al., 2012). While this article introduces three strategies that may help deal with these technologies indirectly, it is imperative that we begin theorizing resistance more intensely.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This research was supported by the Social Sciences and Humanities Research Council of Canada.

ORCID iD

Nadine Schuurman https://orcid.org/0000-0003-1362-224X

References

American Civil Liberties Union (2015) Florida Stingray FOIA. Available at: https://www.aclu.org/cases/florida-stingray-foia (accessed 8 April 2017).

Amoore L (2014) Security and the incalculable. *Security Dialogue* 45(5): 423–439.

Amoore L and Hall A (2010) Border theatre: On the arts of security and resistance. *Cultural Geographies* 17(3): 299–319.

Armstrong MP and Ruggles AJ (2005) Geographic information technologies and personal privacy. *Cartographica: The International Journal for Geographic Information and Geovisualization* 40(4): 63–73.

AutoEmotive (n.d.) Available at: http://autoemotive.media.mit.edu/ Available at: (accessed 24 November 2016).

Bakker K (2013) Neoliberal versus postneoliberal water: Geographies of privatization and resistance. *Annals of the Association of American Geographers* 103(2): 253–260.

Biddle S (2016) Long-secret Stingray manuals detail how police can spy on phones. Available at: https://theintercept.com/2016/09/12/long-secret-stingray-manuals-detail-how-police-can-spy-on-phones/ (accessed 8 April 2017).

Brunton F and Nissenbaum H (2015) *Obfuscation: A User's Guide for Privacy and Protest*. Cambridge, MA: MIT Press.

Calo R (2016) Can Americans resist surveillance? *The University of Chicago Law Review* 83(1): 23–43.

Campbell H and Heyman J (2007) Slantwise: Beyond domination and resistance on the border. *Journal of Contemporary Ethnography* 36(1): 3–30.

de Certeau M (2011) *The Practice of Everyday Life*, 3rd edn, trans. Rendall SF. Berkeley: University of California Press.

Conner-Simons A (2016) Detecting emotions with wireless signals. Available at: https://news.mit.edu/2016/detecting-emotions-with-wireless-signals-0920 (accessed 24 November 2016).

Crampton J (2007) The biopolitical justification for geosurveillance. *Geographical Review* 97(3): 389–403.

Crampton J (2014) Collect it all: National security, big data and governance. *GeoJournal* 80(4). DOI: 10.1007/s10708-014-9598-y.

Crawford K (2016) Can an algorithm be agonistic? Ten scenes about living in calculated publics. *Science, Technology & Human Values* 41(1): 77–92.

Curry MR (1997) The digital individual and the private realm. *Annals of the Association of American Geographers* 87(4): 681–699.

Dalton CM and Thatcher J (2015) Inflated granularity: Spatial 'big data' and geodemographics. *Big Data & Society* 2(2): 1–15.

Deleuze G (1992) Postscript on the societies of control. *October* 59: 3–7.

Dencik L and Cable J (2017) The advent of surveillance realism: Public opinion and activist responses to the Snowden leaks. *International Journal of Communication* 11: 763–781.

Dencik L, Hintz A and Cable J (2016) Towards data justice? The ambiguity of anti-surveillance resistance in political activism. *Big Data & Society* 3(2). DOI: 10.1177/2053951716679678.

Elwood S and Leszczynski A (2011) Privacy, reconsidered: New representations, data practices, and the geoweb. *Geoforum* 42(1): 6–15.

Featherstone D (2003) Spatialities of transnational resistance to globalization: The maps of grievance of the inter-continental caravan. *Transactions of the Institute of British Geographers* 28(4): 404–421.

Foucault M (1995) *Discipline & Punish: The Birth of the Prison*. New York: Vintage.

Gates K (2010) The Tampa 'smart CCTV' experiment. *Culture Unbound: Journal of Current Cultural Research* 2(1): 67–89.

Gilens M and Page BI (2014) Testing theories of American politics: Elites, interest groups, and average citizens. *Perspectives on Politics* 12(3): 564–581.

Goss J (1995) 'We know who you are and we know where you live': The instrumental rationality of geodemographic systems. *Economic Geography* 71(2): 171–198.

Haraway DJ (1991) *Simians, Cyborgs and Women: The Reinvention of Nature*. New York: Routledge.

Hill K (2015) You're being secretly tracked with facial recognition, even in church. Available at: http://fusion.net/story/154199/facial-recognition-no-rules/ (accessed 24 November 2016).

Howe D and Nissenbaum H (n.d.) TrackMeNot. Available at: https://cs.nyu.edu/trackmenot/ (accessed 11 April 2017).

Introna LD and Gibbons A (2009) Networks and resistance: Investigating online advocacy networks as a modality for resisting state surveillance. *Surveillance & Society* 6(3): 233–258.

Ioannidis D, Tzovaras D, Mura GD, Ferro M, Valenza G, Tognetti A and Pioggia G (2012) Gait and anthropometric profile biometrics: A step forward. In: Mordini E and Tzovaras D (eds) *Second Generation Biometrics: The Ethical, Legal and Social Context*. Utrecht: Springer Netherlands, 105–127.

Kafer G (2016) Reimagining resistance: Performing transparency and anonymity in surveillance art. *Surveillance & Society* 14(2): 227–239.

Kalish J (2017) Cryptoparties teach attendees how to stay anonymous online. Available at: http://www.npr.org/sections/alltechconsidered/2017/02/06/513705825/cryptoparties-teach-attendees-how-to-stay-anonymous-online (accessed 4 October 2017).

Kingsbury P and Jones III JP (2009) Walter Benjamin's Dionysian adventures on Google Earth. *Geoforum* 40(4): 502–513.

Kitchin R (1998) Towards geographies of cyberspace. *Progress in Human Geography* 22(3): 385–406.

Kitchin R (2015) Continuous geosurveillance in the 'smart city'. *DIS Magazine*. Available at: http://dismagazine.com/dystopia/73066/rob-kitchin-spatial-big-data-and-geosurveillance/ (accessed 15 April 2018).

Leistert O (2012) Resistance against cyber-surveillance within social movements and how surveillance adapts. *Surveillance & Society* 9(4): 441–456.

Leszczynski A (2015) Geoprivacy. In: Kitchin R, Wilson M and Lauriualt T (eds) *Understanding Spatial Media*. London: SAGE.

Leszczynski A and Elwood S (2015) Feminist geographies of new spatial media. *The Canadian Geographer* 59(1): 12–28.

Lubbers E (2015) Undercover research: Corporate and police spying on activists. An introduction to activist intelligence as a new field of surveillance. *Surveillance & Society* 13(3/4): 338–353.

Mann S and Ferenbok J (2013) New media and the power politics of sousveillance in a surveillance-dominated world. *Surveillance & Society* 11(1/2): 18.

Martin AK, van Brakel RE and Bernhard DJ (2009) Understanding resistance to digital surveillance: Towards a multi-disciplinary, multi-actor framework. *Surveillance & Society* 6(3): 213–232.

Martin K (2016) ACLU sues Tacoma police over hidden Stingray records. Available at: https://web.archive.org/web/20170408214752/http://www.thenewstribune.com/news/local/watchdog/article59776736.html (accessed 8 April 2017).

Marx GT (2003) A tack in the shoe: Neutralizing and resisting the new surveillance. *Journal of Social Issues* 59(2): 369–390.

de Montjoye Y-A, Radaelli L, Singh VK and Pentland A (2015) Unique in the shopping mall: On the reidentifiability of credit card metadata. *Science* 347(6221): 536–539.

Mordini E, Tzovaras D and Ashton H (2012) Introduction. In: Mordini E and Tzovaras D (eds) *Second Generation Biometrics: The Ethical, Legal and Social Context*. Utrecht: Springer Netherlands, 1–19.

Murakami Wood D (2017) Spatial profiling, sorting, and prediction. In: Kitchin R, Lauriault TP and Wilson MW (eds) *Understanding Spatial Media*. London: SAGE.

Naylor L (2017) Reframing autonomy in political geography: A feminist geopolitics of autonomous resistance. *Political Geography* 58: 24–35.

Pickerill J and Chatterton P (2006) Notes towards autonomous geographies: Creation, resistance and self-management as survival tactics. *Progress in Human Geography* 30(6): 730–746.

Pickett BL (1996). Foucault and the politics of resistance. *Polity* 28(4): 445–466.

Piwik (2017) Available at: https://piwik.org/ (accessed 13 April 2017).

Privacy International (n.d.) Metadata. Available at: https://www.privacyinternational.org/node/5 (accessed 9 May 2017).

Rivero D (2015) Florida cops have tracked protesters, suicidal people, and robbers with Stingray devices. Available at: https://web.archive.org/web/20170407175411/https://fusion.net/florida-cops-have-tracked-protesters-suicidal-people-1793845660 (accessed 7 April 2017).

Sanchez A (2009) Facebook feeding frenzy: Resistance-through-distance and resistance-through-persistence in the societied network. *Surveillance & Society* 6(3): 275–293. Available at: http://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/3285 (accessed 15 April 2018).

Schneier B (2014) Metadata = surveillance. Available at: https://web.archive.org/web/20160521134529/https://www.schneier.com/blog/archives/2014/03/metadata_survei.html (accessed 14 April 2017).

Schultz D (n.d.) Internet Noise. Available at: https://web.archive.org/web/20170410182649/https://slifty.github.io/internet_noise/index.html (accessed 11 April 2017).

Schuurman N (2000) Trouble in the heartland: GIS and its critics in the 1990s. *Progress in Human Geography* 24(4): 569–590. DOI: 10.1191/030913200100189111.

Schuurman N (2002) Women and technology in geography: a cyborg manifesto for GIS. *The Canadian Geographer/Le Géographe Canadien* 46(3): 258–265.

Schuurman N (2004) Databases and bodies: A cyborg update. *Environment and Planning A* 36(8): 1337–1340. DOI: 10.1068/a3608_b.

Scott JC (1987) *Weapons of the Weak: Everyday Forms of Peasant Resistance*. New Haven: Yale University Press.

Seglins D, Braga M and Cullen C (2017) RCMP reveals use of secretive cellphone surveillance technology for the first time. Available at: https://web.archive.org/web/20170407164535/http://www.cbc.ca/news/technology/rcmp-surveillance-imsi-catcher-mdi-stingray-cellphone-1.4056750 (accessed 7 April 2017).

Smith S (2017) ISP data pollution. Available at: https://github.com/essandess/isp-data-pollution (accessed 11 April 2017).

Snowdon W (2016) ‘It’s creepy’: Edmonton police backtrack on StingRay surveillance, but expert calls for more oversight. Available at: https://web.archive.org/web/20170408221854/http://www.cbc.ca/news/

canada/edmonton/edmonton-police-backtrack-on-stringray-surveillance-statement-1.3721648 (accessed 8 April 2017).

Sparke M (2008) Political geography – political geographies of globalization III: Resistance. *Progress in Human Geography* 32(3): 423–440. DOI: 10.1177/0309132507086878.

Swanlund D and Schuurman N (2016) Mechanism matters: Data production for geosurveillance. *Annals of the American Association of Geographers*. DOI: 10.1080/24694452.2016.1188680.

The Guardian (2015) FBI operating fleet of surveillance aircraft flying over US cities. Available at: https://web.archive.org/web/20170407172431/https://www.theguardian.com/us-news/2015/jun/02/fbi-surveillance-government-planes-cities (accessed 7 April 2017).

US Department of Homeland Security (2014) Future attribute screening technology. Available at: https://www.dhs.gov/publication/future-attribute-screening-technology (accessed 22 November 2016).

Waddell K (2017) An algorithm that hides your online tracks with random footsteps. *The Atlantic*. Available at: https://www.theatlantic.com/technology/archive/2017/04/hiding-the-signal-in-the-noise/522564/ (accessed 16 April 2017).

Wilson MW (2009) Cyborg geographies: Towards hybrid epistemologies. *Gender, Place & Culture* 16(5): 499–516. DOI: 10.1080/09663690903148390.

Zetter K (2015) Feds admit stingrays can disrupt cell service of bystanders. Available at: https://web.archive.org/web/20170408222231/https://www.wired.com/2015/03/feds-admit-stingrays-can-disrupt-cell-service-bystanders/ (accessed 8 April 2017).

Zetter K (2016) California police used stingrays in planes to spy on phones. Available at: https://web.archive.org/web/20170407172434/https://www.wired.com/2016/01/california-police-used-stingrays-in-planes-to-spy-on-phones/ (accessed 7 April 2017).

Author biographies

David Swanlund is a PhD student at Simon Fraser University. His research interests are in geospatial privacy protection and geosurveillance.

Nadine Schuurman is a Professor of Geography at Simon Fraser University. Her research interests are at the intersection of health geography and GIS, as well as critical GIS.