Geosurveillance, Biometrics, and Resistance

by

David Swanlund

B.A. (Hons.), Simon Fraser University, 2016

Thesis Submitted in Partial Fulfillment of the

Requirements for the Degree of

Master of Arts

in the

Department of Geography

Faculty of Environment

SIMON FRASER UNIVERSITY

Fall 2017

Approval

Name:	**David Swanlund**
Degree:	**Master of Arts**
Title:	**Geosurveillance, Biometrics, and Resistance**
Examining Committee:	**Chair:** **Jason Leach** Assistant Professor
	Nadine Schuurman Senior Supervisor Professor
	Paul Kingsbury Supervisor Professor
	Sarah Elwood External Examiner Professor Department of Geography University of Washington
Date Defended/Approved:	December 11, 2017

Abstract

Geosurveillance is continually evolving to achieve a wider reach and finer granularity. This thesis has two objectives: to understand (1) how biometric technologies could shape the evolution of geosurveillance, and (2) how we can begin resisting geosurveillance before this evolution occurs. The former is based on new second-generation biometrics, which analyze physiological traits, often wirelessly, to calculate stress levels, emotions, and health conditions. Because they work on the body itself from a distance, they hold the potential to both intensify and extend geosurveillance, making it more difficult to resist. The latter objective takes up this topic of resisting geosurveillance, which is otherwise absent within the geographical literature. It surveys tactics and strategies that would enable meaningful resistance to geosurveillance as it operates today. Finally, it concludes that both short-term tactics and long-term strategies are integral to resistance, but that biometrics will require a more strategic approach in the future.

Keywords: surveillance; resistance; biometrics; security; privacy

Acknowledgements

This thesis would not be possible without the help and support of my supervisor, Nadine Schuurman, as well as those that served on my committee, Paul Kingsbury and Sarah Elwood. This research was also generously funded by the Social Sciences and Humanities Research Council of Canada.

To my friends and lab mates, Blake Byron Walker, Michael Martin, Tatenda Makanga, and Leah Rosenkrantz, thank you for not only your support, but all the coffees, burritos, beers, walks, runs, hikes, board games, and good conversations.

Most of all, Aateka, you have endured more this year than I have in my entire life. Thank you for not just your love and support, but your constant inspiration.

Table of Contents

List of Tables

List of Figures

Chapter 1.

Introduction

On November 3rd 2017, the iPhone X was released. The phone had been generating significant attention since its announcement in September, particularly regarding its departure from Touch ID, the well-known fingerprint reader Apple had used on previous iPhones (Brandom, 2017; Heisler, 2017). Instead, Apple opted for Face ID, a facial recognition system meant to unlock users' phones just by looking at them. Immediately surrounding the release, fans began to try and outsmart the new system, quickly finding that it could (sometimes) be fooled by identical twins or highly detailed masks of the phone owner's face (Fingas, 2017; Hern, 2017; Mimoso, 2017; Ulanoff, 2017). The media frenzy that ensued was quickly tamped out by others noting how rare these scenarios are for most users, and in fact suggest that Face ID is relatively secure (Goodin, 2017). As such, Face ID is shaping up to be a similar success to what its fingerprint-based predecessor was. Apple can boast a one in one million false acceptance rate, bringing consumers strong security without the hassle of passwords or pin-codes (Apple, 2017).

Face ID is just one of the many examples where biometrics have been integrated into consumer-oriented technologies and then accepted into everyday life (M. Campbell, 2016; Microsoft, n.d.; Samsung, n.d.). Yet the biometrics that consumers regularly interact with are relatively mundane; they merely verify who we are to unlock our devices. They are simple, convenient, and actively protect our privacy rather than intrude upon it. There exists, however, another side of biometrics that the public is not as in touch with. New biometric technologies are asking much deeper questions with significant consequences for privacy. They can measure our physiology, and in doing so can discover how stressed we are, what emotions we may be feeling, and can uncover what health conditions we may be suffering, even those we are unaware of (Mordini & Ashton, 2012; Sutrop & Laas-Mikko, 2012). All of this can be accomplished passively and wirelessly from a distance, without us being aware, as we move about the spaces in our daily lives. The potential for surveillance is immense.

This thesis is an attempt to bring more attention to these new technologies, and to explore ways that we can begin enacting resistance to geosurveillance more broadly. It works to

achieve this through a substantive case study and a survey of tools for resistance. What follows in this introduction is a brief overview of the major themes that will be discussed in depth throughout the thesis, before concluding with an overview of the thesis structure.

1.1. Biometrics

The biometrics industry is far larger than the small section of it devoted to unlocking smartphones and laptops. In fact, the biometrics industry earned an estimated $2.4 billion in 2016, less than half of which was from consumer device authentication (Tractica, 2017). Revenues are projected to grow to $15.1 billion by 2025, a 529% increase over 10 years. These figures alone leave little doubt that biometrics will play a significant role in the coming decade. While much of this role may continue to be in the relatively mundane category of consumer device authentication, far more advanced applications are being developed.

Consumer device authentication falls into what is now being termed first generation biometrics, a category necessitated by the stark contrast to new biometric technologies entering the field. As Mordini, Tzovaras and Ashton describe, “second generation biometrics progress from asking who you are (the focus of first generation biometrics) to asking how you are” (Mordini, Tzovaras, & Ashton, 2012, p. 11). This simple modification to the question has a significant impact. No longer are these technologies simply validating identity, which itself can have immense surveillance potential (such as facial recognition), but are beginning to read into our emotional states, stress levels, health conditions, and mental illnesses (Mordini & Ashton, 2012).

Given these capabilities, second generation biometrics are being developed in a variety of areas that include government surveillance, automotive safety, and health monitoring (AutoEmotive, n.d.; Conner-Simons, 2016; Storm, 2017). In each of these applications second generation biometrics are marketed as providing increased safety and security. They operate using a variety of sensors that can measure physiological properties such as heart rate, respiration, body temperature, pheromones, eye movement, vocal fluctuation, body and face movement, and gait (U.S. Department of Homeland Security, 2008). Algorithms then analyze this information and classify the subject accordingly.

Although geographers have already begun to grapple with biometrics, focus has primarily been on first generation technologies, i.e. those that authenticate individuals' identities. Biometrics have often been deployed at international borders in the form fingerprint, body, and/or face scanners, and as a result these have been the sites of analysis for most geographical research (Amoore, 2006; Amoore & Hall, 2009; Häkli, 2007; Pero & Smith, 2014), although there are some exceptions (Nguyen, 2015; Nishiyama, 2015). This research has been unanimously critical of biometrics, and often draws on biopolitical theory when framing biometric practices (Amoore, 2006; Nguyen, 2015; Nishiyama, 2015). Second generation biometrics, however, mark a significant advancement in capability, and therefore more theorization of the technology is warranted.

1.2. Geosurveillance

While biometrics are trending towards ever-more descriptive data about us, this is also characteristic to the broader surveillance regimes and intelligence communities that develop them. General Keith Alexander, former director of the National Security Agency, argued for a 'whole haystack' approach to intelligence gathering, meaning that as much data as possible should be collected and stored in the rare event any of it is ever needed (Nakashima & Warrick, 2013). Significantly, many of these intelligence operations collect some form of spatial data (Schneier, 2014b; Washington Post, n.d.-a; Weston, Greenwald, & Gallagher, 2014), the necessity for which is clear: unlike all other forms of data, spatial data points directly to where a target actually is (Leszczynski, 2015). Knowing this unlocks many other insights as well, such as who they are meeting, the places they travel, etc.

Intelligence communities are hardly the only parties that place a high value on spatial data, however. There are a wide range of commercial applications for location data that range from highly targeted advertising to improving smartphone geolocation. Nordstrom is a fitting example of consumer tracking gone too far: in 2013, Nordstrom used WiFi to track the location of their customers' cell phones as they moved throughout the store (Cohan, 2013). The resulting data helped Nordstrom track how long each individual customer spent inside a department or aisle, and how often customers returned to the store.

Geographers mirror this emphasis on spatial data in surveillance by evoking the term *geosurveillance*, referring broadly to the surveillance of individuals' locations (J. W. Crampton, 2007; Kitchin, 2015; Swanlund & Schuurman, 2016). David Lyon defines surveillance "as any focused attention to personal details for the purposes of influence, management, or control" (Lyon, 2010, p. 1). This may reasonably be adapted to geosurveillance specifically by narrowing its focus to personal *spatial* details. Again, these spatial details are important not only because they lead directly to our bodies, but also because our location histories are fundamentally revealing about our lives, and, as Leszczynski writes, are "seen to constitute definitive proof or evidence of [our] involvement in specific behaviours, activities, or events" (Leszczynski, 2015, p. 9).

Therefore, if geosurveillance were to be conducted using biometric technologies, the result would be a powerful fusion that could generate immensely descriptive data. Indeed, it is easy to see the value of being able to determine an individual's emotions as they move throughout a space. For instance, if Nordstroms had coupled their location tracking with second generation biometrics, they could see not only how long a customer spent in front of a particular product, but the emotions they felt before and after they arrived at the product's location. Alternatively, if airports deployed second generation biometrics, it would be possible to track an individual for indicators of stress as they move throughout the airport. If stress levels were to suddenly and abnormally rise once they reached a security checkpoint, that may be grounds for further interrogation.

What makes these biometric technologies so powerful for geosurveillance, however, is also what makes them dangerous. When second generation biometrics are used to sort individuals at airports, for instance, they do so by measuring physiological indicators for stress, "which are often associated with intent to do harm" (Zetter, 2011); if an individual shows high signs of stress while being asked the purpose of their trip, the assumption is that they are more likely to be hiding something. However, people who are already marginalized may have legitimate reasons to feel stress when being interrogated by the security state. For instance, a Muslim person who has been racially profiled all their life may understandably feel stressed in a security setting.

Of course, geographers have been tracking geosurveillance closely for several decades, although the exact term is rather new. As far back as the early 1970s, Taylor had warned of the privacy dangers of automated cartography and large computer databases (Taylor, 1974). Two decades later, geodemographics entered the spotlight, with scholars pointing to the surveillance potential associated with geographic information systems (GIS), and the implications for personal privacy (Curry, 1997; Goss, 1995). In recent years, analysis of geosurveillance has been quite diverse. Kitchin, for instance, has examined the geosurveillance that is embedded in the smart city movement, arguing that the rush to smart cities has ignored the social consequences that come with continuous and exhaustive geosurveillance (Kitchin, 2015). Leszczynski and Elwood, on the other hand, bring attention to the gendered aspects of geoprivacy and geosurveillance that manifest in new spatial media, such as FourSquare (Leszczynski & Elwood, 2015). Finally, Dalton and Thatcher come full circle by arguing that many of the problems in our modern age of 'big data' are not new, but actually can be traced back to critiques of geodemographics. Nevertheless, while several themes are present here, what connects them is their attempt to grapple with the explosion of geospatial technology that has occurred over a relatively short period of time.

1.3. Resistance

Given the rapid development of geosurveillance technologies as well as the current capabilities and future potentials of biometrics, discussion of resistance is warranted. Within the broader public's discussions of surveillance, the notion of resistance certainly gained prominence following the Snowden leaks. A large number of web users began to adjust their browsing habits in favor of privacy, such as by using more private search engines (Johnston, 2015). At the same time, privacy workshops became more commonplace, offering users lessons on what tools and practices are available for defending against surveillance (Kalish, 2017). Even news agencies are increasingly utilizing the SecureDrop tool, which allows citizens to provide information to journalists while protecting against surveillance (CBC, n.d.; The Guardian, n.d.; The Intercept, n.d.; Washington Post, n.d.-b). SecureDrop does this using the Tor network, which itself is growing at a significant rate as it provides strong anonymity to users worldwide (The Tor Project, 2017). Even Facebook now has built a version of their website specifically for Tor users

(Facebook, 2016). Indeed, the dangers of mass surveillance are clearly rising in the public consciousness, and polling reflects this (Madden & Rainie, 2015).

Within the geographical literature, however, resisting geosurveillance has gained considerably less attention. To date, there has not been an article that focuses its attention primarily on resisting geosurveillance. Within the broader surveillance studies literatures, there has been more work related to resistance (Brunton & Nissenbaum, 2015; Calo, 2016; Lucas D. Introna & Gibbons, 2009; A. K. Martin, Brakel, & Bernhard, 2009; Marx, 2003). However, one surveillance studies scholar still suggests that resistance is a concept that is 'underdeveloped' (A. K. Martin et al., 2009). This underdevelopment can be attributed to the fact that in surveillance studies and geography alike the focus is overwhelmingly on the dangers of surveillance rather than resistance against it, leading to a comparative lack of research (Dubrofsky & Magnet, 2015; Goss, 1995; Lucas D. Introna & Gibbons, 2009; Kitchin, 2015; Swanlund & Schuurman, 2016).

1.4. Thesis Structure

This introductory chapter is followed by three other chapters in the thesis. The second chapter interrogates a project by the US government to explore the implications of second generation biometrics for geosurveillance and geoprivacy. It argues that second generation biometrics will both intensify and extend geosurveillance due to their topology and spatial characteristics. Furthermore, it argues that this amplified level of surveillance will be disproportionately felt by already-marginalized people. With these future developments for geosurveillance in mind, the third chapter surveys the tools that are available to begin resisting geosurveillance as it exists today. It suggests that both tactics and strategies are needed to meaningfully resist geosurveillance, and that they are mutually reinforcing rather than mutually exclusive. These two chapters are standalone articles that were originally written for publication in peer-reviewed journals. Finally, the fourth chapter concludes the thesis by summarizing and synthesizing the themes present throughout the two main chapters, explicating its contributions, and suggesting directions for future work.

1.5. References

Amoore, L. (2006). Biometric borders: Governing mobilities in the war on terror. Political Geography, 25(3), 336–351. https://doi.org/10.1016/j.polgeo.2006.02.001

Amoore, L., & Hall, A. (2009). Taking People Apart: Digitised Dissection and the Body at the Border. Environment and Planning D: Society and Space, 27(3), 444–464. https://doi.org/10.1068/d1208

Apple. (2017). Face ID Security. Retrieved from https://images.apple.com/business/docs/FaceID_Security_Guide.pdf

AutoEmotive. (n.d.). AutoEmotive. Retrieved November 24, 2016, from http://autoemotive.media.mit.edu/

Brandom, R. (2017, September 12). iPhone X will unlock with facial recognition instead of home button. Retrieved November 23, 2017, from https://www.theverge.com/2017/9/12/16270352/apple-iphone-x-home-button-removed-unlock-touch-id

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

Calo, R. (2016). Can Americans Resist Surveillance? The University of Chicago Law Review, 83(1), 23–43. Retrieved from http://www.jstor.org.proxy.lib.sfu.ca/stable/43741590

Campbell, M. (2016). Average iPhone user unlocks device 80 times per day, 89% use Touch ID, Apple says. Retrieved November 23, 2017, from http://appleinsider.com/articles/16/04/19/average-iphone-user-unlocks-device-80-times-per-day-89-use-touch-id-apple-says

CBC. (n.d.). CBC Secure Drop. Retrieved November 23, 2017, from https://securedrop.cbc.ca/

Cohan, P. (2013). How Nordstrom Uses WiFi To Spy On Shoppers. Retrieved November 23, 2017, from https://www.forbes.com/sites/petercohan/2013/05/09/how-nordstrom-and-home-depot-use-wifi-to-spy-on-shoppers/

Conner-Simons, A. (2016). Detecting emotions with wireless signals. Retrieved November 24, 2016, from https://news.mit.edu/2016/detecting-emotions-with-wireless-signals-0920

Crampton, J. W. (2007). The biopolitical justification for geosurveillance. Geographical Review, 97(3), 389–403. https://doi.org/10.1126/science.15.370.195

Curry, M. R. (1997). The Digital Individual and the Private Realm. Annals of the Association of American Geographers, 87(4), 681–699. https://doi.org/10.1111/1467-8306.00073

Dubrofsky, R. E., & Magnet, S. (2015). Feminist surveillance studies. Durham: Duke University Press.

Facebook. (2016). 1 Million People use Facebook over Tor. Retrieved November 23, 2017, from https://www.facebook.com/notes/facebook-over-tor/1-million-people-use-facebook-over-tor/865624066877648/

Fingas, R. F. (2017). Apple's iPhone X passes twin test in early hands-on with Face ID. Retrieved November 23, 2017, from //appleinsider.com/articles/17/10/31/apples-iphone-x-passes-twin-test-in-early-hands-on-with-face-id

Goodin, D. (2017). Hackers say they broke Apple's Face ID. Here's why we're not convinced. Retrieved November 23, 2017, from https://arstechnica.com/information-technology/2017/11/hackers-say-they-broke-apples-face-id-heres-why-were-not-convinced/

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. https://doi.org/10.2307/144357

Häkli, J. (2007). Biometric identities. Progress in Human Geography, 31(2), 139–141. https://doi.org/10.1177/0309132507075358

Heisler, Y. (2017, October 13). World's top Apple insider says every iPhone will abandon Touch ID next year. Retrieved November 23, 2017, from http://bgr.com/2017/10/13/iphone-x-successor-face-id-replacing-touch-id-all-iphones/

Hern, A. (2017, September 27). Apple: don't use Face ID on an iPhone X if you're under 13 or have a twin. The Guardian. Retrieved from http://www.theguardian.com/technology/2017/sep/27/apple-face-id-iphone-x-under-13-twin-facial-recognition-system-more-secure-touch-id

Introna, L. D., & Gibbons, A. (2009). Networks and Resistance: Investigating online advocacy networks as a modality for resisting state surveillance. Surveillance & Society, 6(3), 233–258. Retrieved from http://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/3283

Johnston, C. (2015). DuckDuckGo Traffic Soars in Wake of Snowden Revelations. The Guardian. Retrieved from http://www.theguardian.com/technology/2015/jun/17/duckduckgo-traffic-snowden-revelations

Kalish, J. (2017). Cryptoparties Teach Attendees How To Stay Anonymous Online. Retrieved October 4, 2017, from http://www.npr.org/sections/alltechconsidered/2017/02/06/513705825/cryptoparties-teach-attendees-how-to-stay-anonymous-online

Kitchin. (2015). Continuous Geosurveillance in the “Smart City.” DIS Magazine. Retrieved from http://dismagazine.com/dystopia/73066/rob-kitchin-spatial-big-data-and-geosurveillance/

Leszczynski, A. (2015). Geoprivacy. In R. Kitchin, M. Wilson, & T. Lauriualt (Eds.), Understanding Spatial Media (Pre-Publication). SAGE. Retrieved from http://ssrn.com/abstract=2663162

Leszczynski, A., & Elwood, S. (2015). Feminist geographies of new spatial media. The Canadian Geographer, 59(1), 12–28. https://doi.org/10.1111/cag.12093

Lyon, D. (2010). Surveillance, Power and Everyday Life. In P. Kalantzis-Cope & K. Gherab-Martín (Eds.), Emerging Digital Spaces in Contemporary Society (pp. 1–37). Palgrave Macmillan UK. https://doi.org/10.1057/9780230299047_18

Madden, M., & Rainie, L. (2015, May 20). Americans’ Attitudes About Privacy, Security and Surveillance. Retrieved November 23, 2017, from http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/

Martin, A. K., Brakel, R. E. van, & Bernhard, D. J. (2009). Understanding resistance to digital surveillance: Towards a multi-disciplinary, multi-actor framework. Surveillance & Society, 6(3), 213–232. Retrieved from http://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/3282

Marx, G. T. (2003). A Tack in the Shoe: Neutralizing and Resisting the New Surveillance. Journal of Social Issues, 59(2), 369–390. https://doi.org/10.1111/1540-4560.00069

Microsoft. (n.d.). Windows Hello. Retrieved November 23, 2017, from https://www.microsoft.com/en-ca/windows/windows-hello

Mimoso, M. (2017). Apple iPhone X Face ID Fooled by a Mask. Retrieved November 23, 2017, from https://threatpost.com/apple-iphone-x-face-id-fooled-by-a-mask/128865/

Mordini, E., & Ashton, H. (2012). The Transparent Body: Medical Information, Physical Privacy and Respect for Body Integrity. In E. Mordini & D. Tzovaras (Eds.), Second Generation Biometrics: The Ethical, Legal and Social Context (pp. 257–283). Springer Netherlands. https://doi.org/10.1007/978-94-007-3892-8_12

Mordini, E., Tzovaras, D., & Ashton, H. (2012). Introduction. In E. Mordini & D. Tzovaras (Eds.), Second Generation Biometrics: The Ethical, Legal and Social Context (pp. 1–19). Springer Netherlands. https://doi.org/10.1007/978-94-007-3892-8_1

Nakashima, E., & Warrick, J. (2013, July 14). For NSA chief, terrorist threat drives passion to 'collect it all.' Washington Post. Retrieved from https://www.washingtonpost.com/world/national-security/for-nsa-chief-terrorist-threat-drives-passion-to-collect-it-all/2013/07/14/3d26ef80-ea49-11e2-a301-ea5a8116d211_story.html

Nguyen, N. (2015). Chokepoint: Regulating US student mobility through biometrics. Political Geography, 46, 1–10. https://doi.org/10.1016/j.polgeo.2014.09.004

Nishiyama, H. (2015). Towards a Global Genealogy of Biopolitics: Race, Colonialism, and Biometrics beyond Europe. Environment and Planning D: Society and Space, 33(2), 331–346. https://doi.org/10.1068/d19912

Pero, R., & Smith, H. (2014). In the "Service" of Migrants: The Temporary Resident Biometrics Project and the Economization of Migrant Labor in Canada. Annals of the Association of American Geographers, 104(2), 401–411. https://doi.org/10.1080/00045608.2013.875804

Samsung. (n.d.). Security - Iris Scanner. Retrieved November 23, 2017, from http://www.samsung.com/ca/smartphones/galaxy-s8/security/

Schneier, B. (2014, February 11). Everything We Know About How the NSA Tracks People's Physical Location. The Atlantic. Retrieved from https://www.theatlantic.com/technology/archive/2014/02/everything-we-know-about-how-the-nsa-tracks-peoples-physical-location/283745/

Storm, D. (2017, May 1). MIT device measures walking speed with wireless signals to detect health problems. Retrieved November 23, 2017, from https://www.computerworld.com/article/3193569/emerging-technology/mit-device-measures-walking-speed-with-wireless-signals-to-detect-health-problems.html

Sutrop, M., & Laas-Mikko, K. (2012). From Identity Verification to Behavior Prediction: Ethical Implications of Second Generation Biometrics. Review of Policy Research, 29(1), 21–36. https://doi.org/10.1111/j.1541-1338.2011.00536.x

Swanlund, D., & Schuurman, N. (2016). Mechanism Matters: Data Production for Geosurveillance. Annals of the American Association of Geographers, 1–16. https://doi.org/10.1080/24694452.2016.1188680

Taylor, D. R. F. (1974). The Canadian Cartographer and the Computer: Present Trends and Future Challenges. Cartographica: The International Journal for Geographic Information and Geovisualization, 11(1), 35–44. https://doi.org/10.3138/U731-43JG-23P0-3P5U

The Guardian. (n.d.). The Guardian SecureDrop Server. Retrieved November 23, 2017, from https://securedrop.theguardian.com/

The Intercept. (n.d.). The Intercept Welcomes Whistleblowers. Retrieved November 23, 2017, from https://theintercept.com/source/

The Tor Project. (2017). Users – Tor Metrics. Retrieved November 23, 2017, from https://metrics.torproject.org/userstats-relay-country.html?start=2010-08-25&end=2017-11-23&country=all&events=off

Tractica. (2017). Global Biometrics Market Revenue to Reach $15.1 Billion by 2025. Retrieved November 14, 2017, from https://www.tractica.com/newsroom/press-releases/global-biometrics-market-revenue-to-reach-15-1-billion-by-2025/

Ulanoff, L. (2017). The iPhone X can't tell the difference between identical twins. Retrieved November 23, 2017, from http://mashable.com/2017/10/31/putting-iphone-x-face-id-to-twin-test/

U.S. Department of Homeland Security. (2008). Privacy Impact Assessment for the Future Attribute Screening Technology (FAST) Project. Retrieved from https://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_st_fast.pdf

Washington Post. (n.d.-a). How the NSA is tracking people right now. Retrieved November 23, 2017, from https://www.washingtonpost.com/apps/g/page/world/how-the-nsa-is-tracking-people-right-now/634/

Washington Post. (n.d.-b). SecureDrop. Retrieved November 23, 2017, from https://www.washingtonpost.com/securedrop/

Weston, G., Greenwald, G., & Gallagher, R. (2014). CSEC Used Airport WiFi To Track Canadian Travellers: Edward Snowden Documents. Retrieved from http://www.cbc.ca/news/politics/csec-used-airport-wi-fi-to-track-canadian-travellers-edward-snowden-documents-1.2517881

Zetter, K. (2011). DHS Launches "Minority Report" Pre-Crime Detection Program. Retrieved November 23, 2017, from https://www.wired.com/2011/10/pre-crime-detection/

Chapter 2.

Second Generation Biometrics and the Future of Geosurveillance: A Minority Report on FAST

This paper was co-authored with Nadine Schuurman, and is currently being revised for publication in ACME.

Abstract: Whereas biometrics are typically seen as existing for the purposes of identity verification, they are rapidly moving towards a new paradigm of behavioural analysis and prediction. The Department of Homeland Security's Future Attribute Screening Technology (FAST) is one example of this shift. In this article, we use FAST to explore the implications of new biometric technologies for geosurveillance. We argue that second generation biometrics mark a major shift in the application of geosurveillance due to their spatial and topological nature, and that they are motivated in part by a desire to make bodies more legible. Further, we argue that second generation biometrics both intensify geosurveillance of already marginalized bodies. Finally, we call for more geographical research into biometrics given their rapid development and oncoming proliferation.

2.1. Introduction

> "Why Homeland Security's Pre-Crime Prevention Technology Is a Terrible Idea" (Bosch & Canfield, 2012)
>
> "Terrorist 'pre-crime' detector field tested in United States" (Weinberger, 2011)
>
> "Homeland Security's 'Pre-Crime' Screening Will Never Work" (Furnas, 2012)
>
> "DHS Begins Testing Controversial Pre-Crime FAST System (On the Willing)" (Loftus, 2011)

There is a striking resemblance between the Department of Homeland Security's (DHS) advanced biometric project and the film *Minority Report*. The film, which centers on the notion of stopping crime before it happens (so-called 'pre-crime'), is referred to with near ubiquity in media discussions of Future Attribute Screening Technology, or FAST, a DHS project that employs an array of biometric technologies in order to protect against terrorism. In fact, even the DHS recognizes the connection: when assessing the risks of FAST, the DHS wrote that "Risks are largely based on perception of 'Big Brother,' 'Minority Report,' or other nefarious technique [sic] being used to unnecessarily intrude upon the traveling public's privacy" (U.S. Department of Homeland Security, 2015, p. 47). The more one learns about FAST, the more accurate this comparison appears.

Indeed, FAST's goal is to flag individuals who may harbour 'malintent', which the DHS defines as "the mental state of an individual intending to cause harm to [American] citizens or infrastructure" (U.S. Department of Homeland Security, 2014). Flagged individuals may be taken aside for further screening and interrogation, despite having neither committed a crime nor having declared clear intent to commit a crime. This is not a case of an individual clearly being jittery as they pass through the security check at an airport being pulled aside for further questioning. This is a case in which a machine wirelessly senses not only visible characteristics such as eye movement and facial twitches, but also hidden characteristics such as heart rate, respiration, and body temperature (pheromones have also been considered) to "identify deception and hostile intent in real time", presumably through mathematical calculation (Milgrom-Levin et al., 2008, p. 22; U.S. Department of Homeland Security, 2008). Amoore & Hall

describe biometrics as taking the body apart and visualizing them in a form of 'digitised dissection' (Amoore & Hall, 2009). This is 'digitised dissection' taken to a new level.

This article interrogates FAST to provide insight into imminent technological changes to geosurveillance. While a similar article could most assuredly be written within the wider, aspatial context of surveillance, we direct our sights to the geographical aspects of it because, as we demonstrate, it is in part these geographical aspects that make projects like FAST so troubling. FAST is particularly interesting because it is emblematic of the modern security state insofar as it is built around the fear of the unknown. For example, in a kind of bodily 'Total Information Awareness', it combines as many sensors as possible that might *potentially* predict malintent, fearing that any given factor may not sufficiently evaluate a given individual (Markoff, 2002). It is also interesting because it takes multiple independent surveillance projects, such as facial recognition and wireless heartbeat sensing (which can be used to infer mood), and draws them into a single project that could operate beyond the highly securitized spaces where we would expect to encounter them, such as airports (Milgrom-Levin et al., 2008).

Of course, we do not intend to claim that FAST in its current and literal form will arrive in every shopping mall in the near future, but we wish to evoke its chimeric technological form, its predictive purpose, and its spatial and topological characteristics to sketch a hologram of the impact that biometrics might have on geosurveillance – in the absence of technological restraint or opposition. Thus, it serves as an case study into the potential future impacts of biometrics on geosurveillance.

Recent advances in biometrics constitute a particularly potent form of geosurveillance, due in part to how they operate spatially. Indeed, the deployment of biometrics in geosurveillance operations marks a significant, and in many ways unavoidable, intensification and extension of surveillance that challenges not only notions of privacy and consent, but of control over one's own body and mind. These ramifications are also more likely to be felt by those that are already marginalized due to the methods that new biometrics use to assess risk. This paper consists of four parts. First, we briefly review biometrics in the geographical literature and differentiate between first and second generation biometrics. The second section provides an overview of the FAST program. The third section situates FAST in a larger landscape of geosurveillance technologies to understand both its innovations and shortcomings. Finally,

the last section of the article theorizes biometric projects like FAST in terms of legibility and argues that they both intensify and extend geosurveillance to the detriment of marginalized bodies.

It is worth noting that we treat the accuracy or calculability of these technologies as secondary within the scope of this article. While this issue is central to the algorithmic and biometric literatures, it remains secondary here for three reasons: *(1)* it has been covered extensively, such as in Amoore (2014), Magnet (2011) and Pugliese (2012); (2) those in power can assert that a given technology's accuracy rate is high, despite what activists claim is the 'real' accuracy of that technology; and *(3)* over the long term, critiques of accuracy can be responded to by an application of further engineering. This does not mean that there is not a short term utility to critiques of accuracy (they are, in fact, imperative), only that over the course of many decades a given technology may develop to overcome its critics' concerns.

2.2. Geography and Biometrics

Biometrics are far from being a major topic of discussion amongst geographers, but have also not gone unnoticed. Notable work on biometrics include Amoore & Hall's analysis of the full body scanners installed in airports, where they framed biometrics as a form of 'digitised dissection' that visualize bodies (Amoore & Hall, 2009). Amoore has also examined the use of biometrics on borders to identify and sort individuals based on calculated risk as a way to fight the war on terror (Amoore, 2006). A viewpoint from Häkli similarly touches on biometrics at borders and implicates them in a form of symbolic violence (Häkli, 2007). Pero & Smith structure their analysis on the role biometrics play in regulating migrant labor as it crosses borders (Pero & Smith, 2014). Nguyen notably departs from the border and brings her analysis to US schools, which are increasingly being regulated using biometric identification technologies (Nguyen, 2015). Nishiyama does likewise, and focuses a Foucauldian analysis on how biometrics are implicated in a form of modern racism (Nishiyama, 2015).

In other words, geographical work on biometrics has tended to focus on the use of biometrics at the border, such as fingerprint and retinal scanning (Amoore, 2006; Häkli, 2007; Pero & Smith, 2014), as well as on the use of full body scanners (Amoore & Hall, 2009). Additionally, analysis on how biometrics are implicated in judging or sorting individuals tends to

primarily engage with how biometrics are used to identify individuals and link them to other information from which to sort them, rather than how biometric measurements themselves can be used to sort individuals (Amoore, 2006; Häkli, 2007; Nguyen, 2015; Pero & Smith, 2014).

Therefore, geographers have primarily engaged with what are now being termed *first generation biometrics*. First generation biometrics are those that are built around identity verification, that use "simple sensors, able to capture and store some physical features of the object to recognize", such as fingerprints or retinal scans (Ghilardi & Keller, 2012, p. 30). However, "it has become abundantly clear that knowing a person's identity is not sufficient to prevent a threat" (Sutrop & Laas-Mikko, 2012, p. 27). Therefore, second generation biometrics take measuring the body a step further:

> Second generation biometrics progress from asking who you are (the focus of first generation biometrics) to asking how you are; they are less interested in permanent data relating to a pure identity, and more propelled by an individuals' relationship with their environment. What are your intentions and how do you manifest these? (Mordini et al., 2012, p. 11)

Examples of second generation biometrics can include "gait, face dynamics, signature dynamics, human computer interfacing, voice and even odour" (Mordini & Ashton, 2012, p. 262). Moreover, the results of second generation biometric scans can be analyzed to uniquely identify an individual using information such as gait analysis (how people walk), which those in both industry and academia have used to uniquely identify individuals with 99 percent accuracy under favourable conditions (Castro, Marin-Jimenez, Guil, & de la Blanca, 2016; Horizon, 2016). Moreover, multiple second generation biometric readings can be stitched together to increase their reliability of unique identification. Alternatively, second generation biometrics, such as wireless heartbeat analysis (which can be used to infer mood) could be paired with first generation biometrics, such as facial recognition, to anchor intents into identities. Significantly, however, aside from facial recognition, many first generation biometrics require some form of active contact, such as placing a finger on a fingerprint scanner or looking into a retinal scanner, whereas second generation biometrics can largely operate passively from a distance without contact or user interaction (Sutrop & Laas-Mikko, 2012). These passive biometrics are "high on the R&D agenda today, enabling the design of systems that can be applied without people even being aware that they are being identified, registered, or assessed" (Van Der Ploeg, 2012, p. 294). Enter FAST.

2.3. Future Attribute Screening Technology

FAST's first notable mentions in the media were in September 2008 (ABC News, 2008; Angeles, 2008; Barrie, 2008). Since then, various details about the project have trickled out through sources including Freedom of Information Act requests, meeting transcripts, privacy impact assessments, and press releases. Much of the project, however, is still shrouded in secrecy, particularly with regard to its developments over the last few years.

In terms of its core technologies, a 2008 privacy impact assessment that the DHS crafted revealed some specific details, but also introduced some ambiguities. According to the assessment, FAST featured at the time:

> (1) A remote cardiovascular and respiratory sensor to measure heart rate and respiration, which allows for the calculation of heart rate, heart rate variability, respiration rate, and respiratory sinus arrhythmia.
>
> (2) A remote eye tracker, which is a device that uses a camera and processing software to track the position and gaze of the eyes (and, in some instances, the entire head) of a subject. Most eye trackers will also provide a measurement of the pupil diameter.
>
> (3) Thermal cameras that provide detailed information on the changes in the thermal properties of the skin in the face will help assess electrodermal activity and measure respiration and eye movements.
>
> (4) A high resolution video that allows for highly detailed images of the face and body to be taken so that image analysis can determine facial features and expressions and body movements, and an audio system for analyzing human voice for pitch change.
>
> (5) Other sensor types such as for pheromones detection are also under consideration. (U.S. Department of Homeland Security, 2008, p. 4)

Unfortunately, this document is from 2008, and there is no recent indication of what 'other sensors' are under consideration in its current stage of development.

Figure 1: **A slide from a DHS presentation providing a visual representation of FAST and outlining its use-cases and capabilities. Source: (Burns, 2007)**

Visual representations of FAST (Figure 1) show it to be a series of rooms that an individual passes through while being interviewed along the way (Burns, 2007; PublicIntelligence, 2012). Whether in the future FAST, or any other derivative projects, will be able to process a single individual, several individuals, or a crowd simultaneously is difficult to know for certain. It is likely that certain aspects of FAST, such as facial or body movement recognition, could be scaled up significantly if deployed in more open environments, but that other aspects could not, such as pheromones or vocal response. Obviously, scaling the technology such that it does not utilize personal interviews would lower the stress response that FAST relies on, thereby reducing its accuracy.

This trade-off between screening depth versus speed could be decided based on the where the technology is deployed, as the ultimate purpose of FAST is to bring to public events a similar level of security to what is achieved in airports. This is revealed by a transcript of a DHS workshop, where the Under Secretary of the DHS Science and Technology Directorate said that

in developing FAST "the goal here is in a public event, like the Super Bowl or the Olympics, to go ahead and see if, can we do this noninvasive screening that will give us indication of hostile intent so that we can take an individual to secondary screening?" (Milgrom-Levin et al., 2008, p. 25). The transcript also alludes to using FAST to secure transit infrastructure such as trains and buses. Again, whether this happens with FAST itself is unknown, but these statements certainly shed light on the perspective and motivations of the DHS in its desire to deploy second generation biometrics in wider, more public settings.

Finally, the DHS sells FAST as a "gender, culture and age-neutral" technology that "does not connect physiological data to an individual, nor does it permanently store collected data once the analysis is complete" (U.S. Department of Homeland Security, 2014). It is worth noting that this statement leaves open the potential to store data for a limited duration (which could mean that data is stored for hours, months, or years, so long as it is not 'permanent'), and that physiological data is inherently tied to the individual from which it is derived. With these openings in mind, it is worth questioning how data collected from FAST may be used in the event of a terror attack, or how it may be used to train the algorithms behind the technology. Nevertheless, if this attempt to distance the technology from "perception[s] of 'Big Brother,' 'Minority Report,' or other nefarious technique[s]" were to be believed (U.S. Department of Homeland Security, 2015, p. 000047), FAST still fits within David Lyon's definition of surveillance "as any focused attention to personal details for the purposes of influence, management, or control" (Lyon, 2010, p. 1), which in this case would be to manage and control individuals who pass through the system as they attempt to enter an airport, Olympic game, etc. Indeed, the DHS is developing a powerful set of technologies that could have significant consequences if ever abused.

2.4. Situating FAST

In order to understand what makes FAST so concerning, it is important to understand the technological landscape in which FAST exists. To do this, we briefly outline a schema of geosurveillance technology by exploring two distinctions within it, one topological and one spatial, which are exemplified in Table 1. Our understanding of topology in this context aligns with GIScience and mathematics, and we therefore focus our attention to the configuration of links and nodes at work in geosurveillance (Bian, 2009; University of Waterloo, 2015). As such,

the topological distinction is between typical geosurveillance technologies that include a mechanism of two-way communication between a receiver and transmitter (we will call this dyadic geosurveillance for clarity), versus what might be termed biometric geosurveillance. This latter category of watching breaks the dyad of receiver and transmitter, and instead enacts a form of geosurveillance that is technologically one sided, insofar as it works on the body itself.

The spatial distinction we have made is between types of geosurveillance that operate *within* space versus those that operate *over* space, which we will refer to as spatial versus spatialized forms of geosurveillance, respectively. These are types of surveillance that geolocate an individual to a discrete location versus those that operate continuously over space. While these two cross-cutting dichotomies may be obvious for some, we must clearly and systematically delineate them to emphasize how they could amplify the operation of geosurveillance, which will potentially shift and redefine privacy.

Table 1: Examples of the cross-cutting topological and spatial categories of geosurveillance. Cells with a darker shade represent the most topologically and spatially efficient forms of geosurveillance.

	IN SPACE	OVER SPACE
DYADIC GEOSURVEILLANCE	GeoIP; Debit/Credit Card Transactions; Social Media Check-ins;	Cell Phone; RFID; GPS
BIOMETRIC GEOSURVEILLANCE	Fingerprint Scanners; Retinal Scanners	Gait Analysis; Facial Recognition; Heartbeat Detection

Dyadic geosurveillance encompasses most geosurveillance technologies that we are familiar with. Those that operate in space might be exemplified by debit or credit card transactions. These geolocate individuals based on a single and discrete point of contact, the store at which the transaction occurred, with active participation on the part of the individual. A less active, but still ultimately voluntary example may include GeoIP, which approximates an internet user's location based on a variety of measurements, but does so in both discrete physical and virtual space. Indeed, this is a fairly mundane form of geosurveillance: while it generates massive volumes of data, this data is sporadic and bound to a single location (e. g., a store at which a purchase was made or an approximate location at which a computer accessed the internet).

On the other hand, those forms of dyadic geosurveillance that operate *over* space can generate much more detailed and continuous data that are not bound to a single location, and instead can be measured remotely. For example, a cell phone can be tracked continuously over space so long as it has reception. Note as well that ultimately both types of dyadic geosurveillance are easily subverted: an individual can pay with cash, can hide their IP address using Tor or a VPN, or can turn off their phone. Of course, there are many social constraints and forces that can prevent this subversion, and these constraints play out differently depending on context and social difference. For instance, a wealthy individual can much more easily use cash to make purchases than a marginalized person reliant on credit to afford groceries between paycheques. From a mere technical perspective, however, subversion is straightforward.

Biometric geosurveillance, however, is much more technically difficult to subvert. Here, examples of biometric technologies that operate within space include fingerprint and retinal scanners, where any locational information that is derived from them will refer only to a specific and singular location in space, such as a particular airport that an individual may travel through. Technologically speaking, they are extremely difficult to subvert due to their measurement of the body itself (hence their deployment in airports), and therefore subversion requires complete avoidance of the technology.

The difficulty of subversion is drastically amplified when spatialized biometrics enter the field. With spatialized biometrics, practical subversion is infeasible due to their ability to operate passively at a distance combined with their non-reliance on individuals carrying some form of receiver (in a way, the individual *becomes* the receiver). For example, to avoid facial recognition one would have to wear a mask (which may not be possible, such as in banks), and even then gait recognition may be able to identify them.

When spatialized biometrics are using second generation technologies, the infeasibility of subversion becomes far more problematic due to the added stakes involved. Again, second generation biometrics work on the body so that they can detect physiological attributes (including heart rate, respiration, gait, and vocal frequency) that enable calculated inferences, including mood. However, these measurements could also be used to detect certain medical conditions. According to Mordini & Ashton, second generation biometrics could potentially detect mental illness such as depression and anxiety, as well as physical conditions such as joint

disorders (Mordini & Ashton, 2012). In short, spatialized biometrics are not only incredibly difficult to subvert, when second generation biometrics are involved they also put our own health privacy at risk of exposure.

Given the dangers of spatialized biometrics, we must also be aware of the related developments being made in both the public and private sector. One active project at MIT aims to use WiFi signals to monitor respiration and heart rate and then infer mood, which can "detect emotions with 70 percent accuracy even when it hadn't previously measured the target person's heartbeat", with accuracy rates rising to 87% with prior data (Conner-Simons, 2016). Another project called AutoEmotive, also at MIT, uses both contact and non-contact sensors to detect drivers' physiological traits in order to measure stress. This information is then used to compensate for the added risk of a stressful driver, such as by increasing headlight strength, warning the driver of their stressful state, or playing relaxing music (AutoEmotive, n.d.). Even churches are beginning to deploy facial recognition to track who is skipping out on the Sabbath (Hill, 2015), while music festivals use the same technology to track spending (Pulliam-Moore, 2015). All the while, the FBI has repurposed photos from drivers licenses to feed into its facial recognition database of over 400 million photos (Kravets, 2016). There is little doubt that these technologies are popular and will be retained and expanded in the near future.

2.5. Theorizing Second Generation Biometrics

At their core, biometrics are tools that render bodies legible. Indeed, a legible subject is one that is knowable, predictable, and therefore able to be managed accordingly (L. L. Martin, 2010). As Lauren Martin's (2010) work argues, legibility has become a staple of airport security, where first generation biometric systems, including retinal and fingerprint scanners, have become familiar technologies. These make subjects legible largely by authenticating their identity and tying it to known information about them. In other words, most first generation biometrics operate by anchoring individuals' bodies into their data-doubles (Amoore, 2006). One possible exception to this is full body scanners, which, instead of asking 'who' we are, tend to ask 'what' we are: what are the boundaries of the body and what dangerous objects are potentially hidden around it? 'Who' and 'what' we are, however, provide highly incomplete assessments of risk.

Second generation biometrics mark a new, intensified level of legibility by shifting the question from 'who' or 'what' to 'how' (Mordini et al., 2012). In this way, the information to be read off an individual's body significantly increases in descriptive power; 'who' someone is or 'what' they carry is less descriptive compared to 'how' they are feeling in a given moment as a determination of the potential threat they pose to public safety. For instance, in relation to the modern 'war on terror', knowing someone's identity isn't likely to stop terrorism unless it is combined with other useful information about them (Sutrop & Laas-Mikko, 2012). On the other hand, knowing that they are nervous or anxious because of their heart rate, respiration, and/or body temperature is enough information on its own to prompt further interrogation. Nothing external is required.

Biometric technologies that operate over space – including both first generation and second generation biometrics – extend the reach of surveillance such that more bodies can be made legible. This is seen in the DHS' intended use-cases for FAST, that involve, for example, higher security screening at sporting events without sacrificing throughput. In terms of prospective uses for these technologies, however, their operation over space makes it possible to not just screen individuals faster, but to screen multiple individuals simultaneously. Therefore, second generation biometrics mark not just an *intensification*, but an *extension* of geosurveillance.

At a broader scale, this desire for legibility can be understood through what Rachel Hall calls the *aesthetics of transparency*:

> The aesthetics of transparency belong to a rationality of government that understands security in terms of visibility. The aesthetics of transparency is motivated by the desire to turn the world (the body) inside-out such that there would no longer be any secrets or interiors, human or geographical, in which our enemies (or enemy within) might find refuge (Hall, 2007, pp. 320–321).

These interiors can include not only the inside of a backpack or oral cavity within which dangers might lurk, but the interiors of minds where malintent might slither. Moreover, Hall writes that "the aesthetics of transparency establishes a binary opposition between interiority and exteriority and privileges the external or visible surface over the suspect's word" (Hall, 2007,

p. 321). Trust then is placed only in the sterile, quantitative composite that is our biometric profile. (Hall, 2007, p. 323).

Understood in this context, second generation biometrics turn the interior inside-out such that it becomes externally visible, allowing the aesthetic of transparency to extend its operation into the previously untrusted and inaccessible territory of the mind. With these internal and invisible characteristics of ourselves reified, any attendant security risks become patently apparent. This is accomplished not only by making visible our heart rate, respiration, body temperature, minute vocal fluctuations, gait, and/or minute facial movements, but by analyzing those data using algorithms that quantify and classify our internal emotions such that they too are external and visible. With these at hand, we become legible and transparent, without dangerous interiors or secrets. We become securable insofar as we can be controlled and regulated, but also securitized, insofar as our bodies become mere subjects of security.

Securitization via biometric legibility, however, is neither an innocent nor neutral maneuver. This is made clear by feminist scholars such as Magnet (2011), who points out that biometrics fail more often when analyzing people of color, or those with disabilities. In fact, many suggest that biometrics tend to work best on the stereotypical young, white, blue-eyed male (Browne, 2015; Magdaleno, 2014; Magnet, 2011). Or as Magnet describes, they are designed for "a Goldilocks subject who is 'jussstright'" (Magnet, 2011, p. 31).

One reason for this preference of the 'Goldilocks subject', and a potential problem that many biometric technologies face is their implementation of machine learning, which relies on training data that may be either inadequate or misrepresentative of the population. For instance, Google's image labeling technology gained notoriety after it classified some of its users as "Gorillas" (Zhang, 2015). The users were African American, and the racist classification was made because of how the system 'learned' from its training data, which presumably contained racist content scraped from the web. That Google's system made such an error simply based on its users' faces illustrates what effects similarly mis-trained biometric systems could have.

If this problem were to be solved in the future, concerns over biometrics' impact on marginalized bodies would remain. Because second generation biometrics will be used to recognize stress in the security context (Zetter, 2011), it is likely that those who already face discrimination will display a higher stress response when being questioned by security. For

instance, a Muslim individual may legitimately fear racial profiling by security agents, and therefore display a higher level of stress as they pass through a security checkpoint, causing them to be singled out for further interrogation. Such a systematic bias could also impact those with mental illnesses, such as anxiety disorder, which may result in an elevated stress response in a wide variety of situations.

Of course, security officers already look for behavioural cues that indicate nervousness or stress. However, the intensifying effects of second generation biometrics increase the efficacy of this practice, while the extending effects enable it to be more widespread. Moreover, because the system takes on an appearance of calculated objectivity, and therefore seems devoid of any room for human subjectivity, the 'truth value' of the practice may be exaggerated. As Lucas Introna notes, calculative practices "have a certain moral authority because they are taken to impose objectivity and neutrality in a complex domain" (L. D. Introna, 2015, p. 39).

Decades ago Mark Poster discussed the slim similarities between digital profiles and living, breathing humans (Poster, 1996). He referred to the proliferation of digital financial profiles as "skeletal selves" and correctly commented that none of us would recognize ourselves in these profiles. Biometric surveillance, of course, makes mockery of those distant concerns with its much more extensive profiling. However, the same arguments are relevant. These profiles and assumptions made, based on biometric surveillance, can never capture or fully represent a human being. And the more different someone is from the person who designed the algorithm and the people used to train it, the more likely someone will be classified as 'abnormal'. As argued above, finding fault in the algorithms is not a long term solution as the counter argument will always be that the technology can be improved. However, as Cathy O'Neil argues in *Weapons of Math Destruction* (2016), the algorithm can do a lot of damage before the technology is changed.

FAST'S supposed innocent objectivity as a technology that is "gender, culture and age-neutral" is clearly problematic (U.S. Department of Homeland Security, 2014). As a collection of entirely second generation biometric technologies that operate over space, we argue that FAST foreshadows how future geosurveillance may be both intensified and extended to facilitate the utmost legibility of securitized subjects. Crucially, this shift will not have even-handed effects on all individuals, but rather will affect already marginalized bodies disproportionately.

2.6. Conclusion

In this article, we explored FAST as a collection of second generation biometric technologies that provide useful insight into both DHS priorities and their plans for future surveillance technologies. We argue that the spatial nature of second generation biometrics, as well as the fact that they operate on the body itself rather than some other carried technology, unlock the potential for geosurveillance to be greatly amplified in the near future. More specifically, this amplification of geosurveillance consists of an intensification due to the increased legibility of subjects, as well as an extension due to the technology's ability to analyze several individuals simultaneously over space. This, we argue, is problematic due to its effects on already marginalized bodies, as well as its appearance as of objectivity and moral authority as a calculative practice (L. D. Introna, 2015).

Our contribution in this article is not a new discovery or grand theoretical intervention, but rather a synthesis. Indeed, it provides a more lucid investigation into what we are collectively beginning to understand about the forms of surveillance that are looming on the technological horizon. This article also contextualizes these developments theoretically to better inform us of their social implications.

As such, we call for increased geographical research into biometrics, particularly those second generation biometrics that operate from a distance over space. While first generation biometrics have been well examined in geography, second generation biometrics are notably absent. Although they are largely still in early stages of development, these new technologies can significantly amplify the operation of surveillance, and therefore our analysis of them should not be deferred.

2.7. References

ABC News. (2008, September 18). Anxiety-detecting machines could spot terrorists. Retrieved November 23, 2016, from http://abcnews.go.com/Technology/story?id=5837147&page=1

Amoore, L. (2006). Biometric borders: Governing mobilities in the war on terror. Political Geography, 25(3), 336–351. https://doi.org/10.1016/j.polgeo.2006.02.001

Amoore, L. (2014). Security and the incalculable. Security Dialogue, 45(5), 423–439. https://doi.org/10.1177/0967010614539719

Amoore, L., & Hall, A. (2009). Taking People Apart: Digitised Dissection and the Body at the Border. Environment and Planning D: Society and Space, 27(3), 444–464. https://doi.org/10.1068/d1208

Angeles, B. C. E. in L. (2008, September 23). New airport screening "could read minds." Retrieved from http://www.telegraph.co.uk/news/worldnews/northamerica/usa/3069960/New-airport-screening-could-read-minds.html

AutoEmotive. (n.d.). AutoEmotive. Retrieved November 24, 2016, from http://autoemotive.media.mit.edu/

Barrie, A. (2008, September 23). Homeland Security Detects Terrorist Threats by Reading Your Mind [Text.Article]. Retrieved November 23, 2016, from http://www.foxnews.com/story/2008/09/23/homeland-security-detects-terrorist-threats-by-reading-your-mind.html

Bian, L. (2009). Spatial Data Models. In R. Kitchin & N. Thrift (Eds.), International Encyclopedia of Human Geography (pp. 337–344). Oxford: Elsevier. https://doi.org/10.1016/B978-008044910-4.00417-X

Bosch, T., & Canfield, D. (2012, April 18). Why Homeland Security's Pre-Crime Prevention Technology Is a Terrible Idea. Slate. Retrieved from http://www.slate.com/blogs/future_tense/2012/04/18/future_attribute_screening_technology_homeland_security_s_minority_report_program_.html

Browne, S. (2015). Dark Matters. Duke University Press. Retrieved from https://doi.org/10.1215/9780822375302

Burns, B. (2007). Future Attribute Screening Technology Mobile Module. Presented at the S&T Stakeholders Conference. Retrieved from https://info.publicintelligence.net/DHS-FAST.pdf

Castro, F. M., Marin-Jimenez, M. J., Guil, N., & de la Blanca, N. P. (2016). Automatic learning of gait signatures for people identification. ArXiv:1603.01006 [Cs]. Retrieved from http://arxiv.org/abs/1603.01006

Conner-Simons, A. (2016). Detecting emotions with wireless signals. Retrieved November 24, 2016, from https://news.mit.edu/2016/detecting-emotions-with-wireless-signals-0920

Furnas, A. (2012, April 17). Homeland Security's "Pre-Crime" Screening Will Never Work. The Atlantic. Retrieved from http://www.theatlantic.com/technology/archive/2012/04/homeland-securitys-pre-crime-screening-will-never-work/255971/

Ghilardi, G., & Keller, F. (2012). Epistemological Foundation of Biometrics. In E. Mordini & D. Tzovaras (Eds.), Second Generation Biometrics: The Ethical, Legal and Social Context (pp. 23–47). Springer Netherlands. https://doi.org/10.1007/978-94-007-3892-8_2

Häkli, J. (2007). Biometric identities. Progress in Human Geography, 31(2), 139–141. https://doi.org/10.1177/0309132507075358

Hall, R. (2007). Of Ziploc Bags and Black Holes: The Aesthetics of Transparency in the War on Terror. The Communication Review, 10(4), 319–346. https://doi.org/10.1080/10714420701715381

Hill, K. (2015). You're Being Secretly Tracked With Facial Recognition, Even in Church. Retrieved November 24, 2016, from http://fusion.net/story/154199/facial-recognition-no-rules/

Horizon. (2016). CCTV software identifies people by their walk. Retrieved November 23, 2016, from http://horizon-magazine.eu/article/cctv-software-identifies-people-their-walk_en.html

Introna, L. D. (2015). Algorithms, Governance, and Governmentality: On Governing Academic Writing. Science, Technology & Human Values, 41(1), 0162243915587360-. https://doi.org/10.1177/0162243915587360

Kravets, D. (2016, June 18). Smile, you're in the FBI face-recognition database. Retrieved November 24, 2016, from http://arstechnica.com/tech-policy/2016/06/smile-youre-in-the-fbi-face-recognition-database/

Loftus, J. (2011). DHS Begins Testing Controversial Pre-Crime FAST System (On the Willing). Retrieved November 22, 2016, from http://gizmodo.com/5847937/dhs-begins-testing-controversial-pre-crime-fast-system-on-the-willing

Lyon, D. (2010). Surveillance, Power and Everyday Life. In P. Kalantzis-Cope & K. Gherab-Martín (Eds.), Emerging Digital Spaces in Contemporary Society (pp. 1–37). Palgrave Macmillan UK. https://doi.org/10.1057/9780230299047_18

Magdaleno, J. (2014, February 4). Is Facial Recognition Technology Racist? Retrieved November 12, 2017, from https://creators.vice.com/en_us/article/53wp3k/is-facial-recognition-technology-racist

Magnet, S. (2011). When biometrics fail: gender, race, and the technology of identity. Durham: Duke University Press.

Markoff, J. (2002, November 9). Threats and Responses: Intelligence; Pentagon Plans a Computer System That Would Peek at Personal Data of Americans. The New York Times. Retrieved from http://www.nytimes.com/2002/11/09/us/threats-responses-intelligence-pentagon-plans-computer-system-that-would-peek.html

Martin, L. L. (2010). Bombs, bodies, and biopolitics: securitizing the subject at the airport security checkpoint. Social & Cultural Geography, 11(1), 17–34. https://doi.org/10.1080/14649360903414585

Milgrom-Levin, T., Teufel, H., Cohen, J., Jensen, D., Landesberg, M., Cate, F. H., … Wright, R. Department of Homeland Security Meeting: "Implementing Privacy Protections in Government Data Mining (2008). Retrieved from https://www.dhs.gov/xlibrary/assets/privacy/privacy_datamining_July24_2008_minutes.pdf

Mordini, E., & Ashton, H. (2012). The Transparent Body: Medical Information, Physical Privacy and Respect for Body Integrity. In E. Mordini & D. Tzovaras (Eds.), Second Generation Biometrics: The Ethical, Legal and Social Context (pp. 257–283). Springer Netherlands. https://doi.org/10.1007/978-94-007-3892-8_12

Mordini, E., Tzovaras, D., & Ashton, H. (2012). Introduction. In E. Mordini & D. Tzovaras (Eds.), Second Generation Biometrics: The Ethical, Legal and Social Context (pp. 1–19). Springer Netherlands. https://doi.org/10.1007/978-94-007-3892-8_1

Nguyen, N. (2015). Chokepoint: Regulating US student mobility through biometrics. Political Geography, 46, 1–10. https://doi.org/10.1016/j.polgeo.2014.09.004

Nishiyama, H. (2015). Towards a Global Genealogy of Biopolitics: Race, Colonialism, and Biometrics beyond Europe. Environment and Planning D: Society and Space, 33(2), 331–346. https://doi.org/10.1068/d19912

O'Neil, C. (2016). Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. Retrieved August 28, 2017, from https://www.amazon.com/Weapons-Math-Destruction-Increases-Inequality/dp/0553418815

Pero, R., & Smith, H. (2014). In the "Service" of Migrants: The Temporary Resident Biometrics Project and the Economization of Migrant Labor in Canada. Annals of the Association of American Geographers, 104(2), 401–411. https://doi.org/10.1080/00045608.2013.875804

Poster, M. (1996). Databases as Discourse, or Electronic Interpellations. In D. Lyon & E. Zureik (Eds.), Computers, Surveillance, and Privacy. Retrieved from http://readinglists.warwick.ac.uk/items/767FD110-73BD-3041-5332-F36BA62ACB3D.html

PublicIntelligence. (2012). Future Attribute Screening Technology (FAST) Promotional Video. Retrieved from https://www.youtube.com/watch?v=48FuWeF4m7U

Pugliese, J. (2012). Biometrics: Bodies, Technologies, Biopolitics (Reprint edition). London: Routledge.

Pulliam-Moore, C. (2015). Download Music Festival Comes Under Fire for Scanning People's Faces, Tracking Their Spending Habits. Retrieved November 24, 2016, from http://fusion.net/story/152495/download-music-festival-comes-under-fire-for-scanning-peoples-faces-tracking-their-spending-habits/

Sutrop, M., & Laas-Mikko, K. (2012). From Identity Verification to Behavior Prediction: Ethical Implications of Second Generation Biometrics. Review of Policy Research, 29(1), 21–36. https://doi.org/10.1111/j.1541-1338.2011.00536.x

University of Waterloo. (2015, October 16). What is Topology? Retrieved December 15, 2017, from https://uwaterloo.ca/pure-mathematics/about-pure-math/what-is-pure-math/what-is-topology

U.S. Department of Homeland Security. (2008). Privacy Impact Assessment for the Future Attribute Screening Technology (FAST) Project. Retrieved from https://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_st_fast.pdf

U.S. Department of Homeland Security. (2014). Future Attribute Screening Technology. Retrieved November 22, 2016, from https://www.dhs.gov/publication/future-attribute-screening-technology

U.S. Department of Homeland Security. (2015). Electronic Privacy Information Center Freedom of Information Act Request Filed to the Department of Homeland Security. Retrieved from https://epic.org/foia/dhs/fast/14-10-14-DHS-FOIA-20150511-DHS-Production.pdf

Van Der Ploeg, I. (2012). Security in the Danger Zone: Normative Issues of Next Generation Biometrics. In E. Mordini & D. Tzovaras (Eds.), Second Generation Biometrics: The Ethical, Legal and Social Context (pp. 287–303). Springer Netherlands. https://doi.org/10.1007/978-94-007-3892-8_13

Weinberger, S. (2011). Terrorist "pre-crime" detector field tested in United States. Nature News. https://doi.org/10.1038/news.2011.323

Zetter, K. (2011). DHS Launches "Minority Report" Pre-Crime Detection Program. Retrieved November 23, 2017, from https://www.wired.com/2011/10/pre-crime-detection/

Zhang, M. (2015). Google Photos Tags Two African-Americans As Gorillas Through Facial Recognition Software. Retrieved August 15, 2017, from http://www.forbes.com/sites/mzhang/2015/07/01/google-photos-tags-two-african-americans-as-gorillas-through-facial-recognition-software/

Chapter 3.

Resisting Geosurveillance: A Survey of Tactics and Strategies for Spatial Privacy

This paper was co-authored with Nadine Schuurman, and was recently revised for publication in Progress in Human Geography

Abstract: Geosurveillance is continually intensifying, as ever-more 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.

3.1. Introduction

On April 5, 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, Braga, & Cullen, 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 (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 geosurveillance, 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" (p.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, as it can integrate a wide range of other theoretical tools and can be easily operationalized. 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 & 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.

3.2. 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 & Elwood, 2015), the problems inherent to geodemographics and their continued relevance to spatial big data (Dalton & 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 & Ruggles, 2005; J. W. Crampton, 2007; Elwood & Leszczynski, 2011; Leszczynski, 2015; Murakami Wood, 2017; Swanlund & 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 & 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 our research may not be exhaustive, we have yet to encounter an article in which the central, explicit theme was resisting geosurveillance. 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 (L. Dencik, Hintz, & Cable, 2016; Lucas D. Introna & Gibbons, 2009). There is a noted disconnect between those activists who resist surveillance, and those that are subject to it (L. 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 (Lucas D. Introna & 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 & Ferenbok, 2013, p. 18). These examples should serve as a reminder of the incompleteness of power. Indeed, as Pickett 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 has contributed significant work on resistance, this work may not fully replace or fill in for the kind of spatial perspective that a geographer might contribute.

3.3. 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 do 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" (p.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.

3.3.1. 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 & 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 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.

3.3.2. 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 & 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 & 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% of individuals (Montjoye, Radaelli, Singh, & Pentland, 2015). In this way, spatial obfuscation may be significantly harder than obfuscation of other types.

3.3.3. 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 eleven 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.

3.4. 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.

3.4.1. 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, 2014a). 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 & 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, else the public will continue to resign themselves to the apparent inevitability of geosurveillance.

3.4.2. 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, p. 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.

3.4.3. 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 & 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 (L. 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" (p. 9).

Therefore, data justice unites a wider range of activists around the ways that data, including its collection, use, and representation, is 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.

3.5. Discussion

If, as Foucault asserted, that 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 suggests 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" (p.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; U.S. 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" (p.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 retheorization of resistance, our taxonomy of tactics and strategies points in the direction that we believe such a retheorization 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 challenging broader 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 nor 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.

3.6. 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.

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 significant 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.

3.7. References

American Civil Liberties Union. (2015). Florida Stingray FOIA. Retrieved April 8, 2017, from https://web.archive.org/web/20170408214756/https://www.aclu.org/cases/florida-stingray-foia

Amoore, L. (2014). Security and the incalculable. Security Dialogue, 45(5), 423–439. https://doi.org/10.1177/0967010614539719

Amoore, L., & Hall, A. (2010). Border theatre: on the arts of security and resistance. Cultural Geographies, 17(3), 299–319. https://doi.org/10.1177/1474474010368604

Armstrong, M. P., & Ruggles, A. J. (2005). Geographic Information Technologies and Personal Privacy. Cartographica: The International Journal for Geographic Information and Geovisualization, 40(4), 63–73. https://doi.org/10.3138/RU65-81R3-0W75-8V21

AutoEmotive. (n.d.). AutoEmotive. Retrieved November 24, 2016, from http://autoemotive.media.mit.edu/

Bakker, K. (2013). Neoliberal Versus Postneoliberal Water: Geographies of Privatization and Resistance. Annals of the Association of American Geographers, 103(2), 253–260. https://doi.org/10.1080/00045608.2013.756246

Biddle, S. (2016). Long-Secret Stingray Manuals Detail How Police Can Spy on Phones. Retrieved April 8, 2017, from https://theintercept.com/2016/09/12/long-secret-stingray-manuals-detail-how-police-can-spy-on-phones/

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

Calo, R. (2016). Can Americans Resist Surveillance? The University of Chicago Law Review, 83(1), 23–43. Retrieved from http://www.jstor.org.proxy.lib.sfu.ca/stable/43741590

Campbell, H., & Heyman, J. (2007). Slantwise: Beyond Domination and Resistance on the Border. Journal of Contemporary Ethnography, 36(1), 3–30. https://doi.org/10.1177/0891241606287000

Certeau, M. de. (2011). The Practice of Everyday Life. (S. F. Rendall, Trans.) (3 edition). Berkeley, Calif.: University of California Press.

Conner-Simons, A. (2016). Detecting emotions with wireless signals. Retrieved November 24, 2016, from https://news.mit.edu/2016/detecting-emotions-with-wireless-signals-0920

Crampton, J. (2014). Collect It All: National Security, Big Data and Governance. GeoJournal, 80(4). https://doi.org/10.1007/s10708-014-9598-y

Crampton, J. W. (2007). The biopolitical justification for geosurveillance. Geographical Review, 97(3), 389–403. https://doi.org/10.1126/science.15.370.195

Crawford, K. (2016). Can an algorithm be agonistic? Ten scenes about living in calculated publics. Science, Technology & Human Values, 41(1), 77–92. https://doi.org/10.1177/0162243915589635

Curry, M. R. (1997). The Digital Individual and the Private Realm. Annals of the Association of American Geographers, 87(4), 681–699. https://doi.org/10.1111/1467-8306.00073

Dalton, C. M., & Thatcher, J. (2015). Inflated granularity: Spatial "Big Data" and geodemographics. Big Data & Society, 2(2), 1–15. https://doi.org/10.1177/2053951715601144

Deleuze, G. (1992). Postscript on the Societies of Control, 59, 3–7.

Dencik, L., & Cable, J. (2017). The advent of surveillance realism: Public opinion and activist responses to the Snowden leaks. International Journal of Communication, 11, 763–781. Retrieved from http://orca.cf.ac.uk/97855/

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

Elwood, S., & Leszczynski, A. (2011). Privacy, Reconsidered: New Representations, Data Practices, and the Geoweb. Geoforum, 42(1), 6–15. https://doi.org/10.1016/j.geoforum.2010.08.003

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. Retrieved from http://www.jstor.org.proxy.lib.sfu.ca/stable/3804389

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

Gates, K. (2010). The Tampa "smart CCTV" experiment. Culture Unbound: Journal of Current Cultural Research, 2(1), 67–89. Retrieved from http://www.cultureunbound.ep.liu.se/article.asp?DOI=10.3384/cu.2000.1525.102567

Gilens, M., & Page, B. I. (2014). Testing Theories of American Politics: Elites, Interest Groups, and Average Citizens. Perspectives on Politics, 12(03), 564–581. https://doi.org/10.1017/S1537592714001595

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. https://doi.org/10.2307/144357

Haraway, D. J. (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. Retrieved November 24, 2016, from http://fusion.net/story/154199/facial-recognition-no-rules/

Howe, D., & Nissenbaum, H. (n.d.). TrackMeNot. Retrieved April 11, 2017, from https://cs.nyu.edu/trackmenot/

Introna, L. D., & Gibbons, A. (2009). Networks and Resistance: Investigating online advocacy networks as a modality for resisting state surveillance. Surveillance & Society, 6(3), 233–258. Retrieved from http://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/3283

Ioannidis, D., Tzovaras, D., Mura, G. D., Ferro, M., Valenza, G., Tognetti, A., & Pioggia, G. (2012). Gait and Anthropometric Profile Biometrics: A Step Forward. In E. Mordini & D. Tzovaras (Eds.), Second Generation Biometrics: The Ethical, Legal and Social Context (pp. 105–127). Springer Netherlands. https://doi.org/10.1007/978-94-007-3892-8_5

Kafer, G. (2016). Reimagining Resistance: Performing Transparency and Anonymity in Surveillance Art. Surveillance & Society, 14(2), 227–239. Retrieved from http://proxy.lib.sfu.ca/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=i3h&AN=119194538&site=ehost-live

Kalish, J. (2017). Cryptoparties Teach Attendees How To Stay Anonymous Online. Retrieved October 4, 2017, from http://www.npr.org/sections/alltechconsidered/2017/02/06/513705825/cryptoparties-teach-attendees-how-to-stay-anonymous-online

Kingsbury, P., & Jones III, J. P. (2009). Walter Benjamin’s Dionysian Adventures on Google Earth. Geoforum, 40(4), 502–513. https://doi.org/10.1016/j.geoforum.2008.10.002

Kitchin, R. (2015). Continuous Geosurveillance in the “Smart City.” Retrieved from http://dismagazine.com/dystopia/73066/rob-kitchin-spatial-big-data-and-geosurveillance/

Kitchin, R. m. (1998). Towards geographies of cyberspace. Progress in Human Geography, 22(3), 385–406. Retrieved from http://proxy.lib.sfu.ca/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=eih&AN=1120886&site=ehost-live

Leistert, O. (2012). Resistance against Cyber-Surveillance within Social Movements and how Surveillance Adapts. Surveillance & Society, 9(4), 441–456. Retrieved from http://proxy.lib.sfu.ca/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=i3h&AN=87532853&site=ehost-live

Leszczynski, A. (2017). Geoprivacy. In R. Kitchin, M. Wilson, & T. Lauriualt (Eds.), Understanding Spatial Media. SAGE. Retrieved from http://ssrn.com/abstract=2663162

Leszczynski, A., & Elwood, S. (2015). Feminist geographies of new spatial media. The Canadian Geographer, 59(1), 12–28. https://doi.org/10.1111/cag.12093

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. Retrieved from http://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/undercover_research

Lyon, D. (2010). Surveillance, Power and Everyday Life. In P. Kalantzis-Cope & K. Gherab-Martín (Eds.), Emerging Digital Spaces in Contemporary Society (pp. 1–37). Palgrave Macmillan UK. https://doi.org/10.1057/9780230299047_18

Mann, S., & Ferenbok, J. (2013). New media and the power politics of sousveillance in a surveillance-dominated world. Surveillance & Society, 11(1/2), 18. Retrieved from http://search.proquest.com/openview/4ea0bcb6787abb7085dfd9b6d54d9edb/1?pq-origsite=gscholar&cbl=396354

Martin, A. K., Brakel, R. E. van, & Bernhard, D. J. (2009). Understanding resistance to digital surveillance: Towards a multi-disciplinary, multi-actor framework. Surveillance & Society, 6(3), 213–232. Retrieved from http://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/3282

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

Marx, G. T. (2003). A Tack in the Shoe: Neutralizing and Resisting the New Surveillance. Journal of Social Issues, 59(2), 369–390. https://doi.org/10.1111/1540-4560.00069

Montjoye, Y.-A. de, Radaelli, L., Singh, V. K., & Pentland, A. “Sandy.” (2015). Unique in the shopping mall: On the reidentifiability of credit card metadata. Science, 347(6221), 536–539. https://doi.org/10.1126/science.1256297

Mordini, E., & Ashton, H. (2012). The Transparent Body: Medical Information, Physical Privacy and Respect for Body Integrity. In E. Mordini & D. Tzovaras (Eds.), Second Generation Biometrics: The Ethical, Legal and Social Context (pp. 257–283). Springer Netherlands. https://doi.org/10.1007/978-94-007-3892-8_12

Mordini, E., Tzovaras, D., & Ashton, H. (2012). Introduction. In E. Mordini & D. Tzovaras (Eds.), Second Generation Biometrics: The Ethical, Legal and Social Context (pp. 1–19). Springer Netherlands. https://doi.org/10.1007/978-94-007-3892-8_1

Murakami Wood, D. (2017). Spatial Profiling, Sorting, and Prediction. In R. Kitchin, T. P. Lauriault, & M. W. Wilson (Eds.), Understanding Spatial Media. SAGE.

Naylor, L. (2017). Reframing autonomy in political geography: A feminist geopolitics of autonomous resistance. Political Geography, 58, 24–35. https://doi.org/10.1016/j.polgeo.2017.01.001

Pickerill, J., & Chatterton, P. (2006). Notes towards autonomous geographies: creation, resistance and self-management as survival tactics. Progress in Human Geography, 30(6), 730–746. https://doi.org/10.1177/0309132506071516

Piwik. (2017). Piwik. Retrieved April 13, 2017, from https://piwik.org/

Privacy International. (n.d.). Metadata. Retrieved May 9, 2017, from https://www.privacyinternational.org/node/53

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

Sanchez, A. (2009). Facebook Feeding Frenzy: Resistance-through-Distance and Resistance-through-Persistence in the Societied Network. Surveillance & Society, 6(3), 275–293. Retrieved from http://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/3285

Schneier, B. (2014). Metadata = Surveillance. Retrieved April 14, 2017, from https://web.archive.org/web/20160521134529/https://www.schneier.com/blog/archives/2014/03/metadata_survei.html

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

Schuurman, N. (2002). Women and technology in geography: a cyborg manifesto for GIS. The Canadian Geographer/Le Géographe Canadien, 46(3), 258–265. Retrieved from http://onlinelibrary.wiley.com/doi/10.1111/j.1541-0064.2002.tb00748.x/abstract

Schuurman, N. (2004). Databases and Bodies: A Cyborg Update. Environment and Planning A, 36(8), 1337–1340. https://doi.org/10.1068/a3608_b

Scott, J. C. (1987). Weapons of the Weak: Everyday Forms of Peasant Resistance (Revised ed. edition). Yale University Press.

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

Smith, S. (2017). ISP Data Pollution. Retrieved April 11, 2017, from https://github.com/essandess/isp-data-pollution

Snowdon, W. (2016). "It's creepy": Edmonton police backtrack on StingRay surveillance, but expert calls for more oversight. Retrieved April 8, 2017, from https://web.archive.org/web/20170408221854/http://www.cbc.ca/news/canada/edmonton/edmonton-police-backtrack-on-stringray-surveillance-statement-1.3721648

Sparke, M. (2008). Political geography -- political geographies of globalization III: resistance. Progress in Human Geography, 32(3), 423–440. https://doi.org/10.1177/0309132507086878

Swanlund, D., & Schuurman, N. (2016). Mechanism Matters: Data Production for Geosurveillance. Annals of the American Association of Geographers, 1–16. https://doi.org/10.1080/24694452.2016.1188680

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

Tractica. (2017). Global Biometrics Market Revenue to Reach $15.1 Billion by 2025. Retrieved November 14, 2017, from https://www.tractica.com/newsroom/press-releases/global-biometrics-market-revenue-to-reach-15-1-billion-by-2025/

U.S. Department of Homeland Security. (2014). Future Attribute Screening Technology. Retrieved November 22, 2016, from https://www.dhs.gov/publication/future-attribute-screening-technology

Waddell, K. (2017). An Algorithm That Hides Your Online Tracks With Random Footsteps. The Atlantic. Retrieved from https://www.theatlantic.com/technology/archive/2017/04/hiding-the-signal-in-the-noise/522564/

Wilson, M. W. (2009). Cyborg geographies: towards hybrid epistemologies. Gender, Place & Culture, 16(5), 499–516. https://doi.org/10.1080/09663690903148390

Zetter, K. (2015). Feds Admit Stingrays Can Disrupt Cell Service of Bystanders. Retrieved April 8, 2017, from https://web.archive.org/web/20170408222231/https://www.wired.com/2015/03/feds-admit-stingrays-can-disrupt-cell-service-bystanders/

Zetter, K. (2016). California Police Used Stingrays in Planes to Spy on Phones. Retrieved April 7, 2017, from https://web.archive.org/web/20170407172434/https://www.wired.com/2016/01/california-police-used-stingrays-in-planes-to-spy-on-phones/

Chapter 4.

Conclusion

Although they have not yet been widely deployed, second generation biometrics are troubling. They can read into our bodies in ways that not long ago may have been considered science fiction. Our emotions, our physical health, and our mental well-being are all within their purview of detection. And yet, geosurveillance in its more simplistic forms is already widespread and seemingly inescapable. Indeed, resistance will never be complete. It will be a constant struggle, a tug-of-war whose contestants and rules are constantly evolving. What matters is not winning, but remaining on our feet, keeping the rope taut so that it does not slip to the other side.

4.1. Thesis Summary

This thesis has argued that because biometric technologies hold immense potential for geosurveillance, it is imperative that resistance is further developed and enacted. More specifically, Chapter 2 argued that the second generation biometric project known as FAST provides immense insight into how biometrics may affect the operation of geosurveillance. It exemplifies how second generation biometrics can be used from a distance and on the body itself to generate powerful data for surveilling and sorting individuals. Significantly, this data contains inherent biases that work to the disadvantage of already marginalized people. Moreover, because they work passively from a distance and on the body itself, it is possible for second generation biometric technologies to track a person's emotions as they move across a space without their knowledge or consent, and without any mechanism to 'opt out' of that surveillance.

Chapter 3 argued for more intense theorization of resistance in both the surveillance and geosurveillance literatures. It emphasized the importance of both tactics and strategies for enacting meaningful surveillance, and surveyed different types of tactics and strategies that could be fruitful. In terms of tactics, data minimization, obfuscation, and manipulation were discussed. These refer to reducing the amount of data one produces, creating 'false' data (noise)

to mask what is your 'real' data trail, and purposefully crafting a data trail to one's own advantage, respectively. Strategically, we suggest that work should be done to destabilize the core assumptions of geosurveillance, to build private alternatives to otherwise intrusive applications, and to strengthen the ability for activists to operate. The list of tactics and strategies was not meant to be exhaustive, but rather was designed to provoke further discussion about resistance.

4.2. Research Contributions

Two primary contributions can be distilled from this thesis. First, it introduces second generation biometric technologies to the geography literature, where they have been otherwise overlooked. Work on biometrics thus far has only engaged with first generation technologies (Amoore, 2006; Amoore & Hall, 2009; Häkli, 2007; Nguyen, 2015). While these engagements have been fruitful, the significant advances made by second generation biometrics demand new theorizations.

Second, and in light of these impending biometric technologies, it calls for more theorization of resistance to geosurveillance, and points in the direction that this theorization should take. Resistance to geosurveillance has received little attention, usually comprising, at most, only a small component of any given article (Goss, 1995; Swanlund & Schuurman, 2016). This thesis brings resistance to the foreground, and begins paving a path away from geosurveillance and towards increased geoprivacy.

Further notable contributions are to be found in the way this thesis frames the topological and spatial aspects of geosurveillance technologies, and in doing so describes their implications for how surveillance operates and how it can be subverted. Additionally, its notion of encouraging slantwise tactics to resist geosurveillance is novel, as these subversive actions may otherwise be overlooked despite their potentially significant effects. The thesis makes its final notable contribution in its application of Michel de Certeau's notion of tactics and strategies to resisting geosurveillance. Although it does not do further theoretical development of the concept, it brings it closer to practice within the context of geosurveillance by introducing several tangible methods for action.

4.3. Future Work

Future work should continue to unpack second generation biometrics, particularly as they apply to other applications. This thesis has focused on their use in government surveillance, but their use in health monitoring, retail environments, and consumer analytics also warrant investigation. More fundamentally, the machine learning algorithms that form the building blocks of second generation biometrics deserve close analysis. When algorithms select their own rules without their engineers being able to understand how those rules are arrived at, significant ethical complications arise, particularly in the context of security (Tufekci, 2017). Finally, it is imperative that we collectively begin thinking about how second generation biometrics can be resisted tactically, if at all. And, if tactical resistance is deemed largely infeasible, we must ask what are the strategies of least resistance for limiting the deployment of these technologies?

4.4. Closing Remarks

The landscape of geosurveillance is changing rapidly, but we must not fall into apathy or acquiescence because of this change. Far more powerful technologies are approaching, leaving little time for us to begin resisting geosurveillance as it exists today. It is not enough to criticize egregious instances of geosurveillance; we must look forward and take action, small or large, tactical or strategic. The cyborg is an active and ongoing writing project, but we can (and must) engage with and write it ourselves, as has been the goal of this thesis (Haraway, 1991). However, this thesis is only one small step forward in what must be a much larger effort.

4.5. References

Amoore, L. (2006). Biometric borders: Governing mobilities in the war on terror. Political Geography, 25(3), 336–351. https://doi.org/10.1016/j.polgeo.2006.02.001

Amoore, L., & Hall, A. (2009). Taking People Apart: Digitised Dissection and the Body at the Border. Environment and Planning D: Society and Space, 27(3), 444–464. https://doi.org/10.1068/d1208

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. https://doi.org/10.2307/144357

Häkli, J. (2007). Biometric identities. Progress in Human Geography, 31(2), 139–141. https://doi.org/10.1177/0309132507075358

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

Nguyen, N. (2015). Chokepoint: Regulating US student mobility through biometrics. Political Geography, 46, 1–10. https://doi.org/10.1016/j.polgeo.2014.09.004

Swanlund, D., & Schuurman, N. (2016). Mechanism Matters: Data Production for Geosurveillance. Annals of the American Association of Geographers, 1–16. https://doi.org/10.1080/24694452.2016.1188680

Tufekci, Z. (2017). We're building a dystopia just to make people click on ads. Retrieved from https://www.ted.com/talks/zeynep_tufekci_we_re_building_a_dystopia_just_to_make_people_click_on_ads