Reclaiming Visual Sovereignty:
A Theoretical Critique of Facial Recognition Technology

by

Justin Tetrault

A thesis submitted to the Faculty of Graduate and Post Doctoral Affairs in partial fulfillment of the requirements for the degree of

Master of Arts

in

M.A. Sociology

Carleton University
Ottawa, Ontario

Abstract

This thesis is a critique of facial recognition (FR) technology contributing to both surveillance studies and the anti-security literature - and pacification theory in particular. In this study I engage in a critical discourse analysis to deconstruct the historical relationship between identification and the human face. I argue that identification is a form of pacification because it translates and compresses the human condition into something which can be subject to police powers, and reduces personal and political expression to categories which can only be articulated through their relationship to security and capital. Therefore, the face, and by extension FR software, can be seen as an extension of the pacification process, as faces provide an efficient and accessible way to translate the human body through the material gaze of security. I conclude, therefore, that challenges to FR technology are best rooted within a more material understanding of identification and surveillance.

Acknowledgements

This thesis would not have been possible were it not for a number of people. Thank you to George Rigakos, for agreeing to supervise this project. Your guidance and insight have been invaluable in helping me articulate my ideas. I would also like to express appreciation for my committee member, Aaron Doyle. Thank you for sharing your wisdom and support throughout my experience in the graduate program; your advice and enthusiasm always kept me on track. Thank you to Alexander Castleton, Brian Clarke, Lydia Dobson, Shayna Gersher, Mahdi Nazemroaya, Steven Nguyen, Derek Silva, Bejamin Todd and Rhys Williams for your comradeship and for helping me retain my sanity throughout this process; I wish you all good luck in your future endeavors. I would like express my gratitude to Heidi Rimke and Kirsten Kramer, who have been extremely supportive throughout my academic career. Thank you for encouraging me to pursue graduate studies and for igniting my passion for critical thinking and 'committing' sociology. I would also like to thank my family and friends, whose words of encouragement mean more than I could ever express on paper. Thank you Dad and Mom, Nana and Granda, for your enthusiasm and for always supporting my decision to take this path. I would also like to extend my thanks to the King family, who welcomed us with open arms upon our arrival here in Ottawa. And to my friends back in Winnipeg, thank you for making me feel right at home, even though you were 2000km away! And thank you to my wonderful wife, Miranda, for sharing this journey with me – through all the ups and downs. Your love, patience and optimism constantly inspired me to push forward.

Table of Contents

Chapter 4: A History of Facial Identification

Chapter 5: Facial Recognition as Pacification

Chapter 6: Conclusions

List of Figures

Figure 1

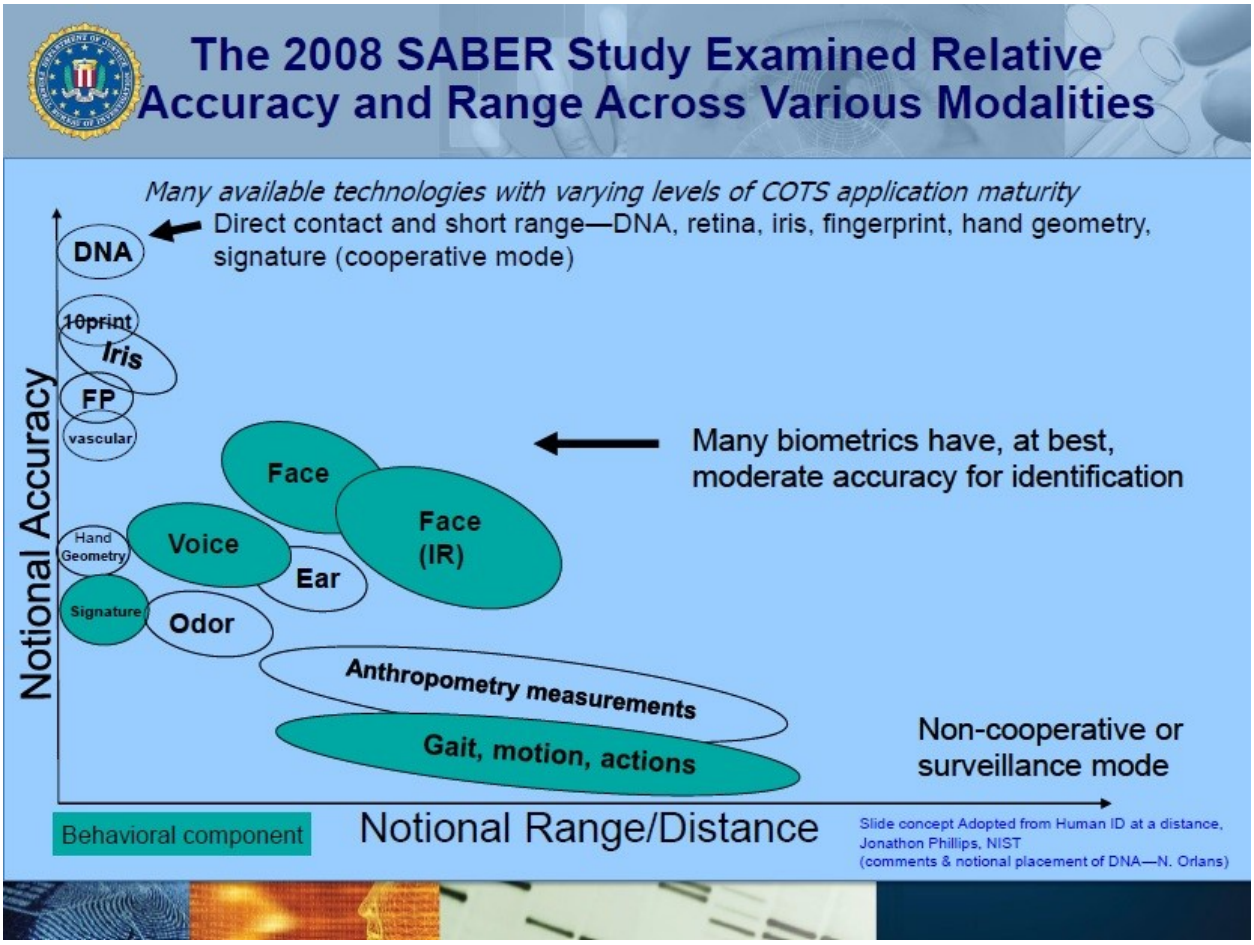


Figure 2

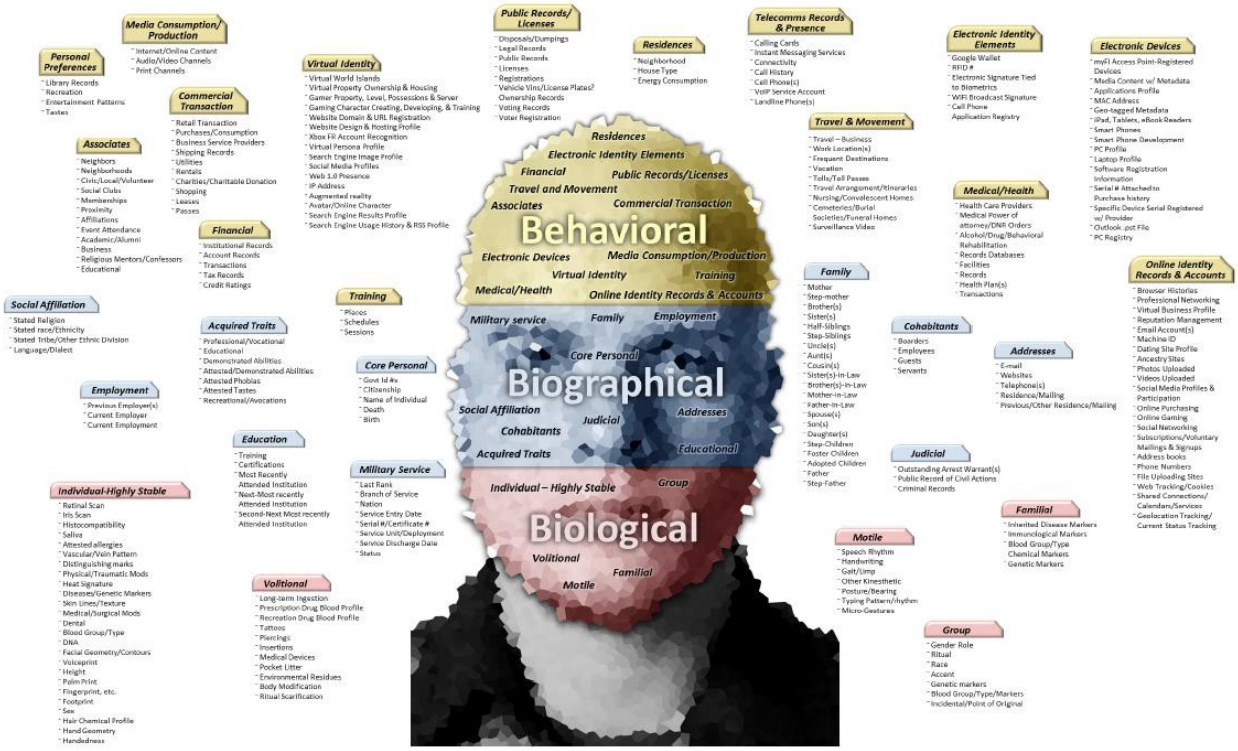
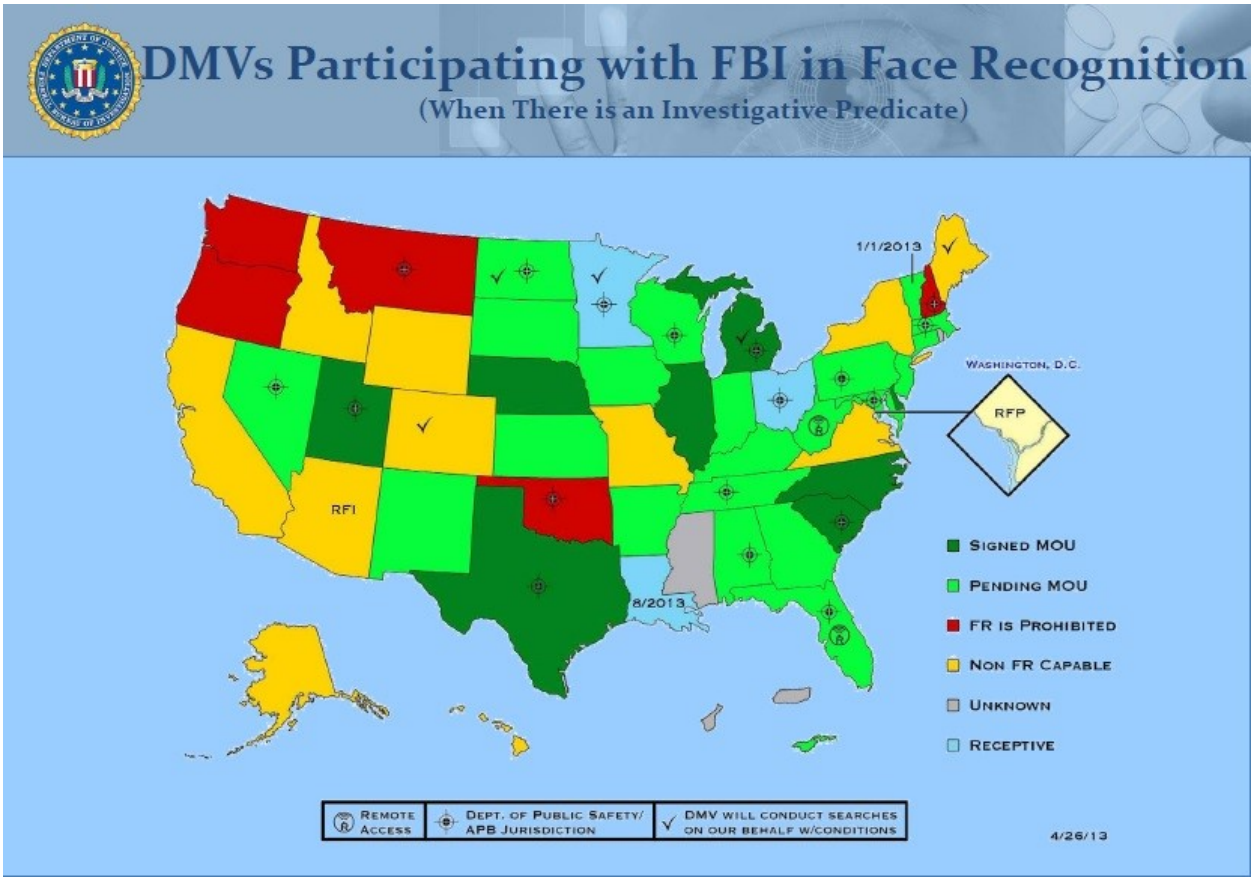

Media Consumption/ Production
Internet/Online Content
Audio/Video Channels
Print Channels
Personal Preferences
Library Records
Recreation
Entertainment Patterns
Tastes
Commercial Transaction
Retail Transaction
Purchases/Consumption
Business Service Providers
Shipping Records
Utilities
Rentals
Charities/Charitable Donation
Shopping
Leases
Passes
Associates
Neighbors
Neighborhoods
Civic/Local/Volunteer
Social Clubs
Memberships
Proximity
Affiliations
Event Attendance
Academic/Alumni
Business
Religious Mentors/Confessors
Educational
Financial
Institutional Records
Account Records
Transactions
Tax Records
Credit Ratings
Social Affiliation
Stated Religion
Stated race/Ethnicity
Stated Tribe/Other Ethnic Division
Language/Dialect
Employment
Previous Employer(s)
Current Employer
Current Employment
Individual-Highly Stable
Retinal Scan
Iris Scan
Histocompatibility
Saliva
Attested allergies
Vascular/Vein Pattern
Distinguishing marks
Physical/Traumatic Mods
Heat Signature
Diseases/Genetic Markers
Skin Lines/Texture
Medical/Surgical Mods
Dental
Blood Group/Type
DNA
Facial Geometry/Contours
Voiceprint
Height
Palm Print
Fingerprint, etc.
Footprint
Sex
Hair Chemical Profile
Hand Geometry
Handedness
Virtual Identity
Virtual World Islands
Virtual Property Ownership & Housing
Gamer Property, Level, Possessions & Server
Gaming Character Creating, Developing, & Training
Website Domain & URL Registration
Website Design & Hosting Profile
Xbox FR Account Recognition
Virtual Persona Profile
Search Engine Image Profile
Social Media Profiles
Web 3.0 Presence
IP Address
Augmented reality
Avatar/Online Character
Search Engine Results Profile
Search Engine Usage History & RSS Profile
Training
Places
Schedules
Sessions
Acquired Traits
Professional/Vocational
Educational
Demonstrated Abilities
Attested/Demonstrated Abilities
Attested Phobias
Attested Tastes
Recreational/Avocations
Education
Training
Certifications
Most Recently Attended Institution
Next-Most recently Attended Institution
Second-Next Most recently Attended Institution
Volitional
Long-term Ingestion
Prescription Drug Blood Profile
Recreation Drug Blood Profile
Tattoos
Piercings
Insertions
Medical Devices
Pocket Litter
Environmental Residues
Body Modification
Ritual Scarification
Public Records/ Licenses
Disposals/Dumpings
Legal Records
Public Records
Licenses
Registrations
Vehicle Vins/License Plates?
Ownership Records
Voting Records
Voter Registration
Residences
Neighborhood
House Type
Energy Consumption
Core Personal
Govt Id #s
Citizenship
Name of Individual
Death
Birth
Military Service
Last Rank
Branch of Service
Nation
Service Entry Date
Serial #/Certificate #
Service Unit/Deployment
Service Discharge Date
Status
Residences
Electronic Identity Elements
Financial
Public Records/Licenses
Travel and Movement
Commercial Transaction
Associates
Behavioral
Electronic Devices
Media Consumption/Production
Virtual Identity
Training
Medical/Health
Online Identity Records & Accounts
Military service
Family
Employment
Core Personal
Biographical
Social Affiliation
Addresses
Judicial
Cohabitants
Educational
Acquired Traits
Individual – Highly Stable
Group
Biological
Volitional
Familial
Motile
Telecomms Records & Presence
Calling Cards
Instant Messaging Services
Connectivity
Call History
Call Phone(s)
VoIP Service Account
Landline Phone(s)
Travel & Movement
Travel – Business
Work Location(s)
Frequent Destinations
Vacation
Tolls/Toll Passes
Travel Arrangement/Itineraries
Nursing/Convalescent Homes
Cemeteries/Burial Societies/Funeral Homes
Surveillance Video
Family
Mother
Step-mother
Brother(s)
Sister(s)
Half-Siblings
Step-Siblings
Uncle(s)
Aunt(s)
Cousin(s)
Sister(s)-in-Law
Brother(s)-in-Law
Mother-in-Law
Father-in-Law
Spouse(s)
Son(s)
Daughter(s)
Step-Children
Foster Children
Adopted Children
Father
Step-Father
Cohabitants
Boarders
Employees
Guests
Servants
Judicial
Outstanding Arrest Warrant(s)
Public Record of Civil Actions
Criminal Records
Motile
Speech Rhythm
Handwriting
Gait/Limp
Other Kinesthetic
Posture/Bearing
Typing Pattern/rhythm
Micro-Gestures
Group
Gender Role
Ritual
Race
Accent
Genetic markers
Blood Group/Type/Markers
Incidental/Point of Original
Electronic Identity Elements
Google Wallet
RFID #
Electronic Signature Tied to Biometrics
WiFi Broadcast Signature
Cell Phone Application Registry
Medical/Health
Health Care Providers
Medical Power of attorney/DNR Orders
Alcohol/Drug/Behavioral Rehabilitation
Records Databases
Facilities
Records
Health Plan(s)
Transactions
Addresses
E-mail
Websites
Telephone(s)
Residence/Mailing
Previous/Other Residence/Mailing
Familial
Inherited Disease Markers
Immunological Markers
Blood Group/Type Chemical Markers
Genetic Markers
Electronic Devices
myFi Access Point-Registered Devices
Media Content w/ Metadata
Applications Profile
MAC Address
Geo-tagged Metadata
iPad, Tablets, eBook Readers
Smart Phones
Smart Phone Development
PC Profile
Laptop Profile
Software Registration Information
Serial # Attached to Purchase history
Specific Device Serial Registered w/ Provider
Outlook .pst File
PC Registry
Online Identity Records & Accounts
Browser Histories
Professional Networking
Virtual Business Profile
Reputation Management
Email Account(s)
Machine ID
Dating Site Profile
Ancestry Sites
Photos Uploaded
Videos Uploaded
Social Media Profiles & Participation
Online Purchasing
Online Gaming
Social Networking
Subscriptions/Voluntary Mailings & Signups
Address books
Phone Numbers
File Uploading Sites
Web Tracking/Cookies
Shared Connections/ Calendars/Services
Geolocation Tracking/ Current Status Tracking

Figure 3


DMVs Participating with FBI in Face Recognition
(When There is an Investigative Predicate)
1/1/2013
WASHINGTON, D.C.
RFP
RFI
8/2013
SIGNED MOU
PENDING MOU
FR IS PROHIBITED
NON FR CAPABLE
UNKNOWN
RECEPTIVE
REMOTE ACCESS
DEPT. OF PUBLIC SAFETY/ APB JURISDICTION
DMV WILL CONDUCT SEARCHES ON OUR BEHALF W/CONDITIONS
4/26/13

Main Body

Chapter 1: Social Context

1.0 Introduction and Social Context

At Super Bowl XXXV in Tampa, Florida in 2001, over one hundred thousand fans had their pictures taken and matched against a computerized police lineup of known criminals, ranging from pickpockets to international terrorists (Chachere 2001). Using a program called 'Facefinder', nineteen individuals - all of whom were petty criminals - were matched against a database created by the Tampa police, the Florida Department of Law Enforcement and the FBI. No one was detained or questioned as the application of the technology was purely experimental, confirming Tampa police spokesman Joe Durkin's suspicion that "these types of criminals would be coming to the Super Bowl to try and prey on the public" (Chachere 2001). The use of facial recognition (FR) software at this event sparked controversy. Critics referred to the episode as the 'Snooper Bowl', and subsequently, the technology has not been reported to have been used at any sporting event following this case. A representative of the International Criminal Police Organization (INTERPOL) has confirmed, however, that FR technology will be utilized at the upcoming FIFA World Cup in 2014 in an effort to stop "World Cup hooligans" (Branchflower 2014). The case of Super Bowl XXXV is one of the earliest public applications of FR software, and since 2001, the technology has purportedly become thirty-times more efficient (see Williams 2007; Bourlai 2014). The technology has penetrated the private sector and the consumer sphere, and has seen increasing demand by state departments and local police. This raises important new questions, not only about

the future of this technology in the social world, but also about the human face's relationship with identification.

Facial recognition technology is a form of biometric surveillance which is programmed to 'see' the human face and connect it to an identity within a database. Due to biometric technology's invasive qualities and historical association with 'deviant' classes, surveillance mechanisms such as fingerprinting and iris scans have largely remained outside of the public sphere, but FR equips pre-existing video surveillance networks with an invisible inspecting gaze which allows a system to potentially identify individuals discreetly, and at a distance. While digital facial recognition has been in development since the 1960s, it has only recently been implemented outside of the laboratory setting, yet the facial recognition market is estimated to grow from $1.92 billion (USD) in 2013 to $6.5 billion in 2018 (Jones 2014). Additionally, in 2012 the FBI invested one billion dollars into an extensive surveillance-identification program which utilizes this technology, and in Canada, passports and driver's license photos are formatted to complement FR software for official government databases (see Vrankulj 2013). The growing popularity and availability of FR technology in the commercial sector raises further questions regarding the potential of FR to operate as a device of social control; one that exploits the consumer data-transparency which saturates Western culture. Criticism of this technology is mounting as Western subjects become increasingly alienated from their own bodies and the technology used to identify them (Denham 2012: 12), yet liberals frame the problem of FR software in the language of privacy, which assumes that photo identification operates in our own interest, neglecting the history of capitalism's colonization of the body (some have also declared the

implementation of FR software as the 'death of anonymity'; see OPC Research Reports 2013: 12; Denham 2012: 11; Danzico 2011; The Economist 2011; Cavoukian and Marinelli 2010). This thesis draws out some of this history and positions the face as an instrument of pacification, facilitated and accelerated by FR technology.

The notion of 'visual sovereignty' refers to an individual's or community's right to visually create a space for self-definition and determination (Raheja 2011). While the concept has been utilized most frequently in works that dismantle the portrayal of negative stereotypes of Indigenous identity in visual culture (particularly in popular films (see Raheja 2011)), this essay is interested in exploring how the visual sovereignty of Western subjects is contested in everyday life through the supremacy of optic security technologies that depend on seeing faces. I will argue that the human face has been deployed as a tool of *pacification* by the liberal state in the form of photo identification, a technology which signifies the non-negotiable marriage of the visualized human body to the state. Facial identification pacifies struggles over visual sovereignty and personal identity by cementing the liberal subject's bondage to the authority of the information database and the increasingly sophisticated gaze of security. This is evident in the fact that the face operates as the *corporeal gatekeeper* to the database, a system which determines who should or should not be included for full access to consumer privileges. Consequently, discrimination based on social inequalities (such as 'race', age, gender and class) has been gradually recast into the mechanical logic of identification. In other words, history and the human condition has been reduced to the individual's immediate relationship to security and capital, a relationship that can be read from the face. This system has been reinforced through the advent of visual mass media – particularly in its

depictions of crime – making discrimination appear as an *a*political, rational calculation. In complementing these existing relationships of power, facial recognition technology can be viewed as the technological apex of visual/optic surveillance, as it theoretically involves crime and deviance being *read* from the body. In addition to being a sophisticated technology of exclusion, FR's ability to exploit the face's relationship to data-flows and digital photo culture (ie: the millions of photos uploaded to social media websites) awards it immense potential to facilitate commerce through fine-grained target advertising, fostering more detailed and efficient forms of discrimination and social control (see chapter 5.2: "Consumer Transparency and Commercial Facial Recognition Technology"). Facial recognition software and all other biometrics are an extension of identity pacification projects, and therefore, resistance to these technologies must transcend the discourse of privacy and begin at the bedrock of liberal identification practices.

The human face has largely escaped serious discussion in sociology; more specifically, the surveillance and governmentality literature have neglected the face's central role in the constitution of official identity, taking for granted the disciplinary power inherent in visualizing this body part. This is problematic as facial features have operated as the central corporeal gatekeeper for information databases throughout the 20th and 21st centuries, those networks which increasingly shape relationships of power, economic transactions and culture. As such, this thesis is interested in providing a framework through which the face can be understood and analyzed politically – as a technology of governance that reproduces unequal relationships of power by making identity and its relationship to the body visible and orderly (as identification), through

which it can then be subject to state and institutional security apparatuses. Under the umbrella of critical realism, this thesis engages with anti-security literature to locate facial identification as a form of pacification. This project is chiefly a theoretical critique of FR technology and facial identification more generally, and subsequently, I will engage in a critical discourse analysis which dismantles these phenomena through a Foucauldian historical analytic (see chapter 2, "Methodology").

The first part of this historical analysis draws from the theories of Deleuze and Guatarri (1987), who posit the face as a political force, illustrating this through its historical relationship to Christian identity – through which they argue, depictions of the face of Jesus Christ formed the bedrock for racist ways of thinking of and seeing the body. It is argued here that the face was traditionally 'seen' in predominantly racialized and gendered terms, until the advent of national-level identity documents through which facial discourse became securitized by the state, although seeing faces through a racialized and gendered lens continued. The following chapter 4.2, "Seizing the Body through Photography", explores the invention of photography and its relationship to law enforcement agencies of the 19th century, through which the body could become visualized and thus captured by the state. Chapter 4.3, "Information Communication Technologies (ICTs) and the Financialization of Identity" looks at the escalating social weight of identification practices through the implementation of CCTV networks in the public sphere, as well as the financialization and monetization of identity – where Western subjects became increasingly defined through their relationship to consumerism and circulations of capital. Chapter 4.4, "Visualizing Risk Through Contemporary Faciality: TV News and War Discourse" explores the hegemony of liberal identification

practices, looking at 21st century cultural reproduction of securitized faces by discussing televisual culture and TV news, using 'digital wanted posters' as an example. This section also examines the overlap of securitized and racialized faces by discussing the role of the face in discourses of crime and war and subsequently, the racialization of 21st century terrorism. The following chapter 4.5, "Frightful Facelessness: Facial Obstruction and Individualism in the Risk Society", examines the cultural implications of the horror film genre, locating it as the cultural culmination of all the above factors - and how the covered face has been constructed as a problem for security. The purpose of chapters 4.4 and 4.5 is to demonstrate how identification practices (projected by dominant culture) become internalized by the majority and may therefore lead to fine-grained forms of self-governance. Chapter 5.0, "Facial Recognition as Pacification", will bring us into the present, problematizing facial recognition technology, through which identity – as defined by the state - can literally be seen through the body. These sections look at the current implementation of FR technology in controlled atmospheres, its utilization by local law enforcement and military (see chapter 5.1 "From the Battlespace to the Gene Pool": Facial Recognition for Military, Borders, and Police"), its potential abuse through the exploitation of data transparency in Western consumer culture (see chapter 5.2 "Consumer Transparency and Commercial Facial Recognition Technology"), and provides a critique of liberal privacy initiatives, offering an alternative way to problematize FR technology (see chapter 5.3 "A Critique of Privacy: Problematizing Facial Recognition Technology"). The concluding chapter 6.0, "Reclaiming Visual Sovereignty: Resisting Facial Recognition Technology", explores the forms of resistance

to FR technology and some of the ways in which individuals and groups have rejected the identification politics of liberal capitalism.

Chapter 2: Methodology

2.0 Introduction & Research Question

This thesis takes facial identification as the primary object of study, particularly in its manifestation as facial recognition technology (or facial biometrics). Using a critical realist meta-theory, these social objects are framed under the logic of *anti-security*, through which facial recognition software can be pinpointed as an extension of the pacification of identity. This thesis seeks to contribute to pacification theory and surveillance studies. For the former, this analysis theorizes the body as a productive enterprise, where ways of seeing and knowing the body become reduced to the individual's relationship to security and consumerism. This process, articulated as facial identification (or photo ID), pacifies struggles over how identity is constructed and how the body is seen and known, limiting forms of resistance. It is important to emphasize here, however, that projects of pacification only *presuppose* resistance and never accomplish it. This implies in my thesis that identification - as a pacification project - is *never* absolute in pacifying dissent, political representation or resistance in self-construction and articulations of identity. As such, it can be stated that facial recognition technology is *not* in and of itself a form of pacification; but rather, like photography and video recording technology before it, FR *can* operate as a potent tool of police and

security projects. For example, FR software would theoretically *not* be a pacifying technology in the hands of activists who are using it to identify agent provocateurs.

To contribute to the latter body of work, surveillance studies, this thesis necessarily develops a materialist conception of the body – bringing a Marxist perspective to surveillance studies. As this essay illustrates, the gaze of optic surveillance – as a disciplinary mechanism - relies heavily on the discourse of facial identification, where the face is reified as a projector of liberal identity. Subsequently, the advent of FR software has led to the commodification of this body part, which is evident in the increasing collection, sharing and selling of biometric information for marketing purposes (see chapter 5.2). In other words, there is a lot of money to be made in the seeing and collecting of faces, as FR software creates opportunities for surplus-value creation (see chapter 5.2).

It should be evident that this thesis utilizes both Foucauldian and Marxist perspectives, a controversial approach that this chapter seeks to resolve by drawing from the works of Hunt (2004), Rigakos and Frauley (2006), and Dupont and Pearce (2001). Drawing from these authors, I situate the ideas of Foucault and Marx under the meta-theory of critical realism, from which a more nuanced theoretical backdrop can used to engage in a critical discourse analysis (CDA) of facial identification. Utilizing this framework, this study draws from inter-disciplinary scholarly research, from anti-psychiatry, visual sociology, the history of photography, news media studies and sociology of the body to literature on policing, security, social control, anarchist theory and surveillance. Primary source data includes information and research gathered from the "Biometrics for Government and National Security" conference that I attended in

Washington DC in February 2014. This event included presentations on (broadly) 'defence biometrics' from notable representatives of various state departments such as the FBI, Department of Defence (DoD), INTERPOL, and the Defence Intelligence Agency (DIA), as well as prominent researchers, specialists and private developers of biometric technology. Other source data in this analysis includes various documents from government agencies and reports from privacy commissioners regarding facial recognition and biometrics more generally (see Denham 2012; Hodai 2013; United State Government Accountability Office 2011; Department of Army 2014; McCall, G., P., Rotenburg, M., Brody D. 2013). While this project is above all a theoretical critique, these sources of data are useful in augmenting the arguments made by my theory. These narratives are important because the public application of FR technology is particularly new, and first-hand institutional accounts and statements made by government officials and marketers are quite revealing as to how and *why* facial biometrics are used (and how they will be applied in the future).

This analysis is therefore guided by the following research question:

> What are the socio-cultural processes and regimes of truth involved in 'seeing' human faces in a way that reproduces dominant relationships of power? What is their relationship to history, the state and 'knowing' the other, and what does it imply for the emerging technology of facial recognition software?

2.1 Critical Realism: Resolving Foucault's Genealogical Method with Marxist Thought

This thesis employs a Foucauldian approach to history as it traces the historical lineage of facial identification as productive enterprise. While this analysis *does* engage with some of the central tenets of the genealogical method, it is not a "genealogy" in the Foucauldian sense. This is because this essay is foremost a theoretical critique of identification and its relationship to the body, an analysis that relies less on first-hand data and more on the dismantling of certain liberal discourses, such as identity, security and privacy. This thesis therefore engages in a critical discourse analysis, as chapter 2.2 "Critical Discourse Analysis (CDA)" will explore in more detail. But first, it is necessary to outline the theoretical implications of the genealogical approach to history, and resolve the perceived contradictions between the ideas of Foucault and Marx.

The genealogical method – in the broadest sense - is an alternative approach to historical analysis and political critique which traces the production (or descent) of knowledge, often for 'those things presumed to have no history' (Rimke 2010: 246). In many ways, Foucault breaks with traditional methodology as the genealogical approach is more than a 'distinct set of rules' (Walters 2012: 117), but also operates as a *critical theory of history*. Deeply critical of traditional historicism, which relies on *naturalized* ontologies in which the "past [is] divorced from the social" (Rimke 2010: 243), Foucault rejects the notion of 'truth' and posits an approach to history which starts "from the decision that universals do not exist" (Foucault 2008: 3). As he delineates:

> Historicism starts from the universal and, as it were, puts it through the grinder of history…Let's suppose that universals do not exist. And then I put the question to history and historians: How can you write history if you do not accept a priori the existence of things like the state, society, the sovereign, and subjects (Foucault 2008: 3)?

Genealogy offers an alternative approach to understanding history, which explicitly contests the 'taken-for-grantedness' of historicism by 'denaturalizing objects and subjects' (Walters 2010: 118). For Foucault (1971), the development of humanity is a *series of interpretations*, and the role of genealogy is to record its history (378). To take the analytic of the 'face' for example, the genealogist would reject the 'natural' existence of the human face, and would proceed to deconstruct the regime of truth that surrounds its very conceptualization – this is one objective of this project.

By rejecting universals and truths the genealogical method involves 'challenges to collective memory', a sort of "counter-memory" which is naturally political (Walters 2012: 125). Thus, more than simply a 'theory' and 'methodology', the application of Foucault's genealogy inevitably employs a political critique. By dissecting the history and discourse of facial identification, for example, the genealogist is immediately invested in a political endeavor which involves countering and critiquing traditional and collective knowledges regarding *why* the face should be associated with identity at all. As such, concerned with the conceptual practices of power (Smith 1990), genealogy often takes science itself as a central referent, as an ideology that can be dissected and deconstructed. Subsequently, the very foundation of the genealogical method contests the most basic convictions of positivist thought, and can therefore be described as an anti-positivist approach. It is important to add here that the analytical aspect of a genealogy

also involves identifying certain *events* of history, which Foucault describes as 'eventalization'. This involves: "[making] visible a *singularity* at places where there is a temptation to invoke a historical constant, an immediate anthropological trait, or an obviousness which imposes itself uniformly on all" (Foucault 1980: 249).

While the logic of Foucauldian theory provides a lucrative pool of thought for analyzing power and history, there are a number of theoretical issues that need to be ironed out. Firstly, Foucault claims that there is no 'natural progression' of society and humanity - knowledge is not something that can be 'complete', and thus, logic is never 'pure'. In Foucault's own words, "critique doesn't have to be the premise of a deduction that concludes 'this, then, is what needs to be done'" (Foucault 2000: 256). For Foucault, a genealogy is a "history of the present" (Foucault 1978: 31) which "does not resemble the evolution of a species and does not map the destiny of a people" (Foucault 1971: 374). However, while Foucault writes at length to distance himself from the traditional histories which elaborate the present 'as the outcome of a teleological progression' (Dupont & Pearce 2001: 134), Foucault's emphasis on self-relflexive discourses and transitions in the 'art of governance' is nonetheless a *grand narrative* (see Hunt 2004; Rigakos & Frauley 2006; Dupont & Pearce 2001). This grand narrative involves a transitory, rational development of history, which is evident in Foucault's various analyses where history and forms of rule unfold as a consequence of rationalizations by self-reflexive governors and their advisors (Dupont & Pearce 2001: 140). Foucault's conceptualization of 'population' is indicative of this approach, through which the notion becomes the logic and organising category utilized by Foucault to "underwrite the transition-passage from the earlier arts of government to later ones – from the reason of

the state to a more autonomous art of governance" (Supont & Pearce 2001: 139). This type of 'evolutionary' or 'progressive' language comprises much of Foucault's historical analysis of the unfolding of liberalism and the art of governance. Importantly this 'rational development of history' – which focuses primarily on dismantling *dominant* discourses - loses sight of historic political struggle, 'particularly the projects of the defeated' (Dupont & Pearce 2001: 134).

Secondly, Foucault's rejection of truth "as a useless notion" (Foucault 1971: 372), is a problematic stance on a number of levels, and the emphasis on this claim has mislead a large body of governmentality studies into interpreting Foucault as an anti-realist philosopher. While some scholars claim that this stance has allowed us to engage in both a 'disconnection and reconnection' with society (Walters 2012: 131), illuminating the previously unseen effects of how "we think about thinking and acting on ourselves and others" (Rimke 2010: 241), the reliance on the perspective that truth is ever only *fabricated*, has led to the idea that one must either declare an 'anti-realism' in order to remain consistent with Foucault's 'intent'; or to drop Foucauldian categories from their analysis altogether, in order to get on with what resembles an 'empirically realist' project (Rigakos & Frauley 2006: 8). Rigakos and Frauley (2006) are right to challenge this distinction as such a dichotomy becomes *anti-theoretical* as it adopts the positivist ontological stance by judging surface content as real – where observable events become the only form of empiricism (Rigakos & Frauley 2006: 9). This is problematic for social science, as to confine observation solely to the monitoring of events leads only to 'endless descriptions of more or less random sequences' (Pawson 1989: 128). The objective however, is to understand 'the underlying mechanism[s] which bring about

particular sequences of events' (Pawson 1989: 128), because events are never discrete, but rather, parts of an object or system. For example, inequalities are not necessarily 'observable' through events, but most certainly exist whether or not we know of their existence; similarly, social institutions such as family, religion, education, work, and law, 'pre-exist our birth and are relatively enduring or *intransitive* and constrain and enable social action' (Rigakos & Frauley 2006: 5, emphasis added). For these reasons, it is more productive to situate Foucauldian thought and the logic of governmentality under the more nuanced lens of critical realism, a philosophy of (social) science and methodology which locates social action as situated activity, conditioned and shaped by social structure (Rigakos & Frauley 2006: 11).

Critical realism is compatible with the genealogical approach as it begins from questions about what exists (ie: the conditions under which social objects such as 'identification' emerge) and then moves toward questions of epistemology, concerned with the production of knowledge about what exists (how can identification be investigated) (Rigakos & Frauley 2006: 6). Methodologically speaking, governmentality is interested in exploring how individuals govern (themselves and others) by the production of truth (Foucault 1980: 256). Critical realism does not reject the Foucauldian argument that truth can be fabricated and produced, but unlike anti-realist governmentality, critical realism posits that there is *probably* a truth as to how those fabrications facilitate, conduct or restrict behavior. Since the production of truth is dependent on relationships of power/knowledge, a genealogy looks closely at the 'series of contingent becomings' that produce knowledge (Walters 2012: 115). In Foucault's (1982) words: "we have to refer to much more *remote processes* if we want to understand

how we have been trapped in our own history" (780, italics added). In contrast to a Marxist analysis for example, a genealogy would involve a 'bottom-up' approach, looking at the descent of facial identification through the dialectical relationship between public discourse and expert or 'official' knowledges. How did dominant culture come to conceptualize the face-identity relationship, and how did expert knowledges help us arrive at its' truth? It is important to note that expert knowledges take a variety of forms, such as through religious experts, medical experts, psychiatric experts, government officials and media experts, etc.; individuals who retain a degree of normalizing power through their knowledge and expertise. Because facial identification is pervasive throughout the social world, this thesis explores its relationship to many of the aforementioned groups. However, this brings us to another critique of Foucault's base ideology, in which much of his work strives to distance itself from concentrated forms of power located in the state and its institutions. This approach to analyzing power – in addition to Foucault's calculated effort to avoid using Marxist terminology - has been perceived as rendering governmentality as incompatible with Marxist thought. However, Foucault nevertheless felt the need to return to the state toward the end of his life and scholars such as Hunt (2004) have argued that Marx and Foucault while different, "are by no means incompatible" (604). Relationships of power, for Foucault, only exist in action; and therefore genealogy entails a commitment to certain *practices* (Walters 20112: 122). As Foucault (1980) explains, "it is a question of analyzing a 'regime of practices' – practices being understood here as what is said and what is done" (248); "practices don't exist without a certain regime of rationality" (Foucault 1980: 251). Marx, like Foucault, is not interested in locating the 'origin' of social objects, but instead, Marx' central focus

is also on social relations and practices (Hunt 2004: 605) – both scholars are interested in how relationships of domination are exercised and reproduced. Even Foucault could not dispense with so-called 'top-down' analyses involving state theory or discussions regarding class, capitalism and the bourgeois, which is particularly evident in some of his later works such as *Security. Territory. Population*. (2007), a book-length treatment of the state under liberalism. While Foucault's (2007) interpretation of the state here emphasizes a *disconnect* between population management, economy, law and police - differing from the Marxist perspective which posits a more unified central power - analytically it is unproductive to restrict analyses of such phenomenon to the dichotomy of a top-down or bottom-up approach that subscribes to one author or the other. Hunt (2004) captures this issue well in the following passage:

> We should not let go of an understanding of the capacity of specific state institutions to condense and mobilize great power resources and capacities. We should avoid any suggestion that there is some methodological rule to guide us. All that can be said is: look to both concentrated and dispersed powers, assume no priority between these, and pay attention to empirical detail (Hunt 2004: 607).

Critical realism provides a nuanced framework from which we can begin to situate social objects from a Foucauldian perspective of history while still retaining a Marxist dialogue (anti-security). As a critical realist project, this thesis takes facial identification as its central object, defines it as a project of pacification, and traces its history as a mechanism of social control through a Foucauldian historical analytic. To reiterate this logic, this thesis does not arrive at a 'truth' regarding how facial identification (and subsequently FR technology) conducts individuals and reproduces inequalities, but instead, hopes to provide methodological suggestions about the questions

to be asked about this phenomenon and where to start with answering them (Hunt 2004: 602). As such, fallibility is a central facet of (critical) realism as this approach insists on the "reflexive need to assess and reassess the social, historical and political situatedness of not only concepts and ideas but the practices that produce and reproduce them" (Rigakos & Frauley 2006: 4). Similarly, Foucault places emphasis on contingency as a main concern of genealogical analysis. For Foucault (1971), knowledge is not something that can ever be complete, and as he asserts, an objective of genealogy is to "[fragment] what was thought unified" (375).

2.2 Critical Discourse Analysis (CDA)

As a theoretical critique, this thesis is interested in deconstructing the taken for granted discourse of liberal identification and its relationship to the face. In order to advance the arguments and ideologies mentioned in the previous chapter, critical discourse analysis will be employed as a way to situate the phenomenon of facial identification as a technology of governance through which the liberal state organizes (or 'makes orderly') the human body for productive purposes.

At the most basic level, CDA can be referred to as a diverse methodological approach which focuses on how discursive practices help produce unequal power relations (Fairclough & Wodak 1997). Often used interchangeably with 'Critical Linguistics' (CL), CDA is a relatively young technique that goes "beyond the description of discourse to an explanation of *how* and *why* particular discourses are produced" (Teo

2000: 11, emphasis in original); and the origin of CDA can be located in a plethora of disciplines and ideologies, from socio-psychology and cognitive science, to socio/applied/and text linguistics and pragmatics (Wodak and Meyer 2009: 1). It is for this reason that CDA acquires its critical dimension. As Wodak and Meyer (2009) explain, it is important here to distinguish CDA from DA as it differs through an "extension of linguistics beyond sentence grammar towards a study of action and interaction" (2, emphasis in original); critical discourse analysts stretch the meaning of discourse from a genre to a register or style, from a building to a political program (Wodak & Meyer 2009: 3). Thus the word 'critical' in CDA signals a departure from the purely descriptive goals of discourse analysts (Sinclair and Coulthard 1975; Stubbs 1983). However, because CDA is interested in 'de-mystifying' and 'unmasking' ideologies (Wodak & Meyer 2009: 3, 8), language remains a central tenet of the approach, as language operates as the primary instrument through which ideology is transmitted, enacted and reproduced (Foucault 1972).

For critical discourse analysts, language is a 'social practice' which Wodak and Meyer (2009) outline in the following passage:

> [Language] is both determined by social structure and contributes to stabilizing and changing that structure simultaneously (7). . .[language] indexes and expresses power, and is involved where there is contention over and a challenge to power (Wodak & Meyer 2009: 10).

Taking this into consideration, CDA must - at some level – operate through a political agenda as all approaches to CDA are 'problem oriented' (Wodak & meyer 2009: 3). For Wodak and Meyer, CDA is interested in illustrating the inequalities that lie in

constructing and communicating discourse. For example, this thesis takes the state narrative of identity and the visualized body (articulated as facial identification) as its central referent, as it is often the case that the most socially consequential discourses involve 'sanitized narratives' (Wodak & Meyer 2009: 19) of the "few talking to the many" (Teo 2000: 44). This is because discourses constructed through institutions, experts and leaders "renders their articulations particularly powerful, authoritative, and ultimately dominant" (Sikka 2006: 110).

As Edkins (1999) argues: "we exist in a world of language, discourse, and ideology, none of which are visible, all of which structure our sense of being and meaning" (cited in Sikka 114). As a practical research method, CDA maintains crucial significance and relevancy today as society becomes increasingly saturated with symbols, images, texts and digital communications that continue to shape the human experience and produce real social consequences. In expanding the scope of discourse, CDA is able to facilitate a flexible research agenda, and is able to adapt to new modes and genres of communication, from developments of interactive communication technologies such as the Internet and video games, to the community narratives of 'transmedia' (Wodak & Meyer 2009: 11). CDA also becomes indispensable in studies of racism and discriminatory discourses as deconstructing dominant ideologies and exposing taken for granted social hierarchies provides an avenue for advocating socially discriminated groups (Wodak & Meyer 2009: 19). This aspect is pertinent to this thesis as discriminatory practices are part and parcel of surveillance regimes and late-modern marketing efforts. Additionally, as a study which focuses on security (policing) and the

body, racism necessarily factors into my discussion, an issue which is explored in chapters 4.1, 4.2, and 4.4.

CDA specializes in power relations and is therefore critical. As Hawkesworth (2006) asserts, a critical foundation is deeply important for researchers as "critical examination of what is most taken for granted can free us from 'the myth of the given' (18); as such, this methodology can be incredibly useful in exposing the role of social values in naturalizing oppressive practices (Hawkesworth 2006: 96). Furthermore, as a politically oriented research practice, CDA's methodological autonomy allows the researcher to complement their interpretations with a political program or take the more cautious route and leave their work open for deliberation. As such, the malleability of CDA as a research practice can be seen as both a positive and negative aspect of the approach. Scholars such as Teo (2000) for example, seek to give CDA 'a conceptual and analytic unity and coherence' (13). Whether this type of clarity is useful for an approach oriented around social issues, is to the discretion of the researcher. CDA does not constitute a well-defined empirical method and there continues to be no 'formal CDA way' of gathering data. CDA is also focused on the hermeneutic tradition than the analytical-deductive tradition (Wodak & Meyer 2009: 27, 28), so while it may be flexible in its ability to draw from both qualitative and quantitative realms, CDA's methodological ambiguities and its strong reliance on interpretation and theory would not satisfy the quantitative purist.

To summarize: utilizing CDA, this thesis seeks to problematize FR technology as a project of pacification, a claim that involves dismantling the discourse of identification which 'naturalizes' the body's relationship to narratives of identity that are most

productive for the status quo. In order to uncover the inequalities produced by this phenomenon, it is required that I explore the historical lineage of the face-identity relationship, something which is best accomplished under a Foucauldian historical analytic, as this approach rejects such naturalized ontologies and therefore offers an approach to history that simultaneously operates as a political critique.

Chapter 3: Identity, Security, Surveillance &Social Control

3.0 Introduction: Literature Review

As Gibbs (2010) posits, much contemporary writing on the body has shown that "the face is a contested surface of the body on which a series of feelings, emotions and affects are most intensely projected, received and circulated" (191 cited in Nigishi 2013: 324); and while the face has been the 'key object of capture within contemporary regimes of surveillance', as Nedishi (2013) puts it (324), this body part has largely been overlooked in sociological discussions of surveillance and identity. The very recent application of facial recognition technology in the public sphere has sparked a dialogue of the role of the face in both classic and contemporary surveillance and security apparatuses, but leaves a lot to be desired in discussions surrounding the vibrant future of biometric identification and the historical role that the face has played in the conduct of conduct. That being said, the literature on facial recognition is very limited – specifically the sociological literature. This is understandable, of course, as the technological capabilities of FR have only recently been sufficient enough to have an impact on social interactions

and everyday life. Only in the last few years has it been anchored as a relatively stable tool for identification in controlled settings (such as in European airports) and as a policing mechanism in various cases across the West, such as the MORIS program – a new portable biometric system used by some US police departments to identify suspects (see chapter 5.1). Less forgivable however, is the lack of discussion on the face's traditional role in liberal governance; the near-absence of this dialogue in surveillance and identity literature is curious when considering the face's central function in state identity documents – there is little talk as to why the state reduces the entire visual of the human body to this singular aspect. The limited literature on these fronts can be seen as a both a weakness and a strength of this project. The central weakness of course lies in the limited pools of knowledge which this analysis can draw from - in regards to specific research, arguments and theories exploring the politics of FR and the face's role in the aforementioned discourses. On the other hand, the sparse research on the face, as the central object of study, can also be seen as a unique opportunity to dissect certain issues and cultural processes by opening up a dialogue through which we can discuss the face as a political force in the West.

3.1 Toward a Theory of Facial Identification as Pacification

Much of the contemporary literature on 'seeing' and recognizing the face is limited to psychological studies and research on neuroperception, which often takes for granted the layers of social construction of the face and its relationship to identity (see chapter 4.1:

"Why the Face?: Seeing, Isolating and Imposing the Human Face"). Subsequently, most literature on facial recognition *technology* focuses on its technical side and/or its implications for privacy; as such, the politics of facial biometrics in these analyses are often neglected or fall under the umbrella of a liberal security logic (see Mockensturm 2002, Introna & Nissenbaum 2010, Denham 2012, Klontz & Jain 2013).

Kelly Gates' 2011 text: *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance* is one of the few accounts that focus on some of the socio-cultural implications and political consequences of facial recognition technology; in Gates (2011) own words: "There are no book-length treatments of the automation of facial recognition…from a social, legal, or critical cultural perspective" (201). As such, Gates' (2011) text provides great insight into the general history, technological mechanics, and current usage of facial biometrics, and Gates, a communications and science studies professor, is critical of the software - problematizing its implementation as a policing mechanism and as a broader technology of governance. Central to Gates' (2011) argument is challenging the claim that FR technology will provide us with more 'more security', a claim, which she argues, is largely unfounded, and that in its current state, the social costs of FR software (which Gates asserts are not yet 'fully understood' but generally fall under the umbrella of 'threats to privacy') far outweigh any perceived benefit that the technology could offer (199). While Gates (2011) largely satisfies these arguments, her problematization of FR software suffers from the circular logic of security, a problem that plagues traditional liberal interpretations of policing and surveillance technology, leaving some of her arguments underdeveloped (see chapter 5.3 for a critique of privacy discourse).

Her study and social critique relies heavily on surveillance theory, drawing from scholars such as Foucault, Lyon and Ericson & Haggerty; however, her application of these theorists is patchy and sometimes inconsistent as she does not provide a clear-cut backdrop through which she frames and problematizes the technology. Discussions surrounding the politics of identification and its relationship to reproducing the status quo is also somewhat lacking. While Gates does draw from certain historical events and external disciplines (such as the psychology of facial expressions), her analysis is largely restricted to the past decade and suffers from an emphasis on the post-9/11 terror hysteria - drawing perhaps too big a line between the pre- and post- 9/11 security complex. As such, a large portion of Gates' text emphasizes FR's role in policing and security in relation to the criminalized other. While this is useful in illustrating FR software in action, it lacks a real critical punch, as Gates (2011) often relies on the problematic concept of 'security' and entertains the liberal mythology of 'balancing' it with the idea of freedom (see 194-198) (for a critique see Neocleous 2007; Neocleous & Rigakos 2011). Some of her primary challenges to FR for example, lie in questioning its potential role in 'providing security', and in 'stabilizing identity' (see 7, 16). Following this mode of thought, the text lacks a discussion of FR's relationship to capital accumulation and there is limited talk of its potential within the realm of consumerism and consumer surveillance. Overall, while this text provides many insights into the capabilities (and limits) of FR software, Gates' analysis leaves a lot to be desired regarding our so-called 'biometric future'. This thesis attempts to fill - what appears to be - a theoretical void of facial biometrics and provide a critical, interdisciplinary and historically grounded analysis of FR technology that escapes the hegemony of liberal security discourse.

While sociological research on FR software is limited, there are many lucrative pools of thought from which we can begin to frame this issue. The following problematizes identification and security and locate them in processes of liberal-order building through which the human body becomes bound to the database system. The historical analysis of this thesis shows how identity – taken as a security mechanism of the state and articulated as identification – has accounted for the problematic of the observable human body, through which the state absorbs those technologies that can *see* and *capture* the body for the purpose of population management. The body, as a visual conveyer of meaning, is a site of chaos, and as the following chapters demonstrate, the liberal state has largely accounted for this issue through *facialization* (see chapter 4.1; Deleuze & Guatarri 1987), where the face becomes the corporeal centerpiece for connecting the tangible subject to state narratives through which the individual can be subject to policing and the disciplinary gaze. This relinquishing of the face is a prerequisite for unhindered movement throughout the institutionalized world of Western societies. The securitization of identity (as something which is articulated by police projects) pacifies political representations of the self and subsequently, the hegemony of identification is often internalized and reproduced by dominant culture (see chapters 4.4 and 4.5). As such, a central theme of this project is the ways in which 'seeing' faces and identity becomes subject to both state narratives of security and productions of dominant culture; two narratives which work together as a reciprocal political force. As Zygmunt Bauman (2001) argues:

> Culture is the activity of making distinctions: of classifying, segregating, drawing boundaries – and so dividing people into categories internally united by similarity and externally separated by difference; and of differentiating the ranges of conduct assigned to the humans allocated to different categories (Bauman 2001: 32).

As consequence, it is often the case that we *see* faces and *know* identities in ways which reproduce certain relationships of power and the status quo (such as through discourses of gendered faces, racialized faces, 'deviant' or 'dangerous' faces – as we will see). To use the language of Deleuze and Guatarri (1987), there is something of an *inhumanity* about the face, which is precisely a symptom of these cultural processes; in other words, these are not *our* faces, these are corporeal instruments of the conduct of conduct, they subject and are subject to categorical stereotypes; *we do not so much have a face as slide into one* (Deleuze & Guatarri 1987: 177). The boundary-drawing obsession of modernity and its emphasis upon 'individualisation' has helped dissolve the notion of identity as a process of *self-construction* to the extent that the self is frequently measured against the totality and its culturally prescribed categories (Bauman 2001). Subsequently, presentation of the self in 'modern living' relies on references to 'standards not of one's making'; the self becomes a "site cleared for norms, laws, ethical rules and courts of justice"; and consequentially, the 'unique other becomes dissolved into the otherness of the Many' (Bauman 2001: 179):

> When the Other dissolves in the Many, the first thing to be washed away is the Face. The Other(s) is (are) now faceless. They are *persons* ('persona' means the mask, and masks hide not disclose faces). I am dealing now with masks (classes, stereotypes, to which the masks/uniforms direct me) not faces. It is the mask which determines whom I am dealing with and what my responses ought to be. I have to learn the meaning of each *kind* of mask and memorize the responses each one calls for (Bauman 2001: 179, italics in original).

Bauman's analogy of the 'washing away' of faces is useful for this analysis, as we can say that cultural productions of the traditional regime of racism, for example, 'washed away' non-white faces through the racializing or 'inferiorizing' of certain facial groups – dissolving entire populations into 'the otherness of the Many' (see chapter 4.1); we can also say this about the Western security complex, which washes away those faces that become subject to forms of state intervention and institutionalization (such as those who are 'wanted', those labelled terrorists, inmates etc.) (see chapter 4.4). And as Bauman poignantly points out in this passage, such a 'washing away' is gradually making-up the very fabric of everyday life – the endless project of order-building subjects Western self-construction to the constraints of identification practices and the culture of individualism (see chapter 4.5). This theme is a central tenet in the anti-security literature as well, as 'the more you can divide and subdivide', the more 'security can colonize all aspects of human practices and thinking' (Rigakos 2011: 62).

Critical security scholars, articulated as 'anti-security', argue, invoking the language of Marx and Engels: "Security is the supreme concept of bourgeois society", this is because the survival of capitalism involves the "constant revolutionizing of production [and the] uninterrupted disturbance of all social conditions" (Marx & Engels cited in Neocleous 2011: 24). Subsequently, the emphasis on security means that at some fundamental level the order of capital is an order of *insecurity* (Rimke 2011: 194). In the words of Marx and Engels: "everlasting uncertainty and agitation distinguish the bourgeois epoch from all earlier ones" (cited in Neocleous 2011: 24). As such, it can be argued that the spectacular insecurities of capitalism fashion it as a system of *dis*order, one which requires the politics of *security* through which the capitalist 'order' is

fabricated, structured and administrated (Neocleous 2011: 24). This notion, termed by Neocleous (2011) as 'the fabrication of social order' – and its relationship to the politics of security - culminates many of the themes discussed in this thesis.

To connect this pool of thought to the subjects of population management and identity, we turn again to Foucault (2007), who has made similar arguments regarding security in some of his later writings on liberal governance and the state, through which he summarizes his work as follows:

> . . . sovereignty is exercised within the borders of a territory, discipline is exercised on the bodies of individuals, and *security is exercised over a whole population* (Foucault 2007: 11, italics added).

In his text, *Security, Territory, Population,* Foucault (2007) asserts that "freedom is nothing else but the correlative of the deployment of apparatuses of security" (48). In other words, you are free to enjoy the fruits of liberal-capitalism, but must subject yourself to the expansive regimes of security through which you must maneuver (assuming of course that you are not disruptive and can contribute to the various circulations of capital). This notion of 'circulations' is important in Foucault's mode of thought as security involves not so much establishing limits and frontiers, or fixing locations, "as above all and essentially, making possible, guaranteeing and ensuring circulations: the circulation of people, merchandise, and air, etcetera." (29). Security "lets things happen", and as such, security apparatuses are deployed upon certain circulations, which involves "organizing, or anyway allowing the development of ever-wider circuits" (45, 49). And interestingly - lecturing years before the advent of literature on the risk society - Foucault points out that threats to these circulations are constructed only as

"important due to [their] probability"; asserting that 'dangerousness is a mechanism of security' and the estimation of probabilities is "pretty much the essential characteristic of the mechanism of security" (Foucault 2007: 7, 20).

Influenced by the Foucauldian pool of thought, anti-security scholars such as Rigakos (2012) explicitly emphasize the politically charged nature of security:

> . . .skin-heads, anarchists, football hooligans, terrorists…are just risk categories, risk groups. But we know security is not apolitical. Although security appears apolitical, it is anything but. Security intelligence is obsessed with understanding the nature of the threat and making determinations about preparedness. The central threat to security, to the capitalist order, is anything that threatens the basis for wealth accumulation under capitalism. . . the history of security is the history of enforcing this system of accumulation (Rigakos 2012): 13).

Thus, to return to the idea of 'order', we can argue as Foucault (2007) does, that "order is what remains when everything that is prohibited has in fact been prevented" (46). Subsequently, we can say that things are 'orderly' if they behave as you have expected them to; "that is if you may safely leave them out of account when planning your actions" (2001: 31). 'Security' then, is what comes "from the ability to predict, with little or no error, what the results of your own actions will be" (Bauman 2001: 31). Thus the order of capitalism, engulfed in a perpetual struggle to quell a myriad of social, political and economic antagonisms, is ceaseless in its deployment of security apparatuses to safeguard circulations of capital and conduct populations in a way that is functional to this order.

It is important to note that the implementation of security as a mode of governance is not something particularly new to the liberal state; Foucault situates the advent of security as part of the art governance through which liberalism began to

problematize the notion of *population* (Foucault 2007), a concept which he describes as follows:

> . . .[populations is] a set of elements in which we can note constants and regularities even in accidents, in which we can identify the universal of desire regularly producing the benefit of all, and with regard to which we can *identify a number of modifiable variables on which it depends* (Foucault 2007: 74, italics added).

We should not be misled by Foucault's language here as 'the benefit of all' must be understood as relative to a certain order; as he explains, liberal governance makes the division between 'good' and 'bad' circulations (order and disorder), and is subsequently interested in maximizing the good circulation by *diminishing the bad* (2007: 18, 46). To elaborate on this some more, the population (as a 'knowable' entity subject to a given circulation) is an *instrument* of the state (Foucault 2007: 106). The wealth, longevity, and health of the state is dependent on the *productivity* of its population, and as such, liberalism involves a certain productive order through which ideas are structured by legal mechanisms, behavior is normalized through discipline, and the circulation of productivity is maximized through apparatuses of security, which allows for certain kinds of freedoms. However, this is not to discount the extensive manipulation involved in population management through which individual and public interests and consciousness is boiled down to the 'benefit of all':

> . . .[the population] is both aware of what it wants and unaware of what is being done to it. Interest as the consciousness of each of the individuals making up the population, and interest as the interest of the population, whatever the individual interests and aspirations may be of those who comprise the population, will be the ambiguous fundamental target and instrument of the government of populations (Foucault 2007: 106).

The above passage is in-step with Bauman's earlier contention that the modern individual must always be understood and articulated in reference to the totality (through which they become dissolved in the otherness of the Many).

Following this assertion that 'individual interests and aspirations' are at once a central 'target' *and* 'instrument' of liberal governance, from here we can begin to see how the 'order' of identity (as identification) plays a key role in the management of populations, through which identity must be fashioned in accordance to the interests of the whole – identity must be made *useful*.

As Bauman (2001) argues:

> The discovery of chaos beefs up the zeal for ordering and the passions that surround the practice of order building, order repairing and order protecting (Bauman 2001: 33).

Identity is arguably one of the most chaotic forms of the human experience as to articulate such a thing involves sorting out every facet of human expression and conduct, such as the visual, linguistics, behavior, ethics, even smell, and subjecting such phenomenon to rigid categorizations through which disciplinary regimes of normality are the referent. This is precisely the project that modernity has undertaken – engaged in a ceaseless process of "creative destruction" (Bauman 2001: 64). Critical scholars such as Stuart Hall (1995), Rosemary Hennessy (2000), and Judith Butler (1993) challenge the

modernizing impulse of liberal-capitalism's identity politics and assert that identity must be understood as performative, discursive, and as a product of historical materialism. Butler (1993) defines identity as follows:

> . . . identifications belong to the imaginary; they are phantasmatic efforts of alignment, loyalty, ambiguous and cross-corporeal cohabitations, they unsettle the I; they are the sedimentation of the 'we' in the constitution of any I, the structuring present of alterity in the very formulation of the I. Identifications are never fully and finally made; they are incessantly reconstituted, and, as such, are subject to the volatile logic of iterability. *They are that which is constantly marshalled, consolidated, retrenched, contested and, on occasion, compelled to give way* (Butler 1993: 105, italics added).

Judith Butler's dismantling of identity in the above passage illustrates the inherent instability of the concept – and as such, the ways in which identity becomes subject to ceaseless production and reproduction in efforts to make it orderly. Identification practices are a definitive part of these efforts, and it is important to emphasize that identity (for the purpose of this essay) is distinct from identification. As the following will delineate, identification involves institutional forces that transform (self-) identity into a technology of governance.

To borrow from Stuart Hall's (1995) language, identities are subject to "radical historicization" and are therefore constantly in the process of change and transformation (4). We can apply this to Foucauldian theory by pinpointing identity's central relationship to the integration of new *security technologies*. As Foucault (2007) argues:

> [For the security apparatus,]. . .*new elements are constantly being integrated*: production, psychology, behavior, the ways of doing things of producers, buyers, consumers, importers, and exporters, and the world market (Foucault 2007: 45, italics added).

Likely trying to avoid the reductionist tendencies of the term, Foucault is of course referring in the above passage to the implementation of new *technologies*, which for him, encompasses both the introduction of hard technologies (as the word 'technology' is traditionally understood) *and* technologies of governance. As Foucault (1984) argues in an earlier piece, government is also a function of technology: "the government of individuals, the government of souls, the government of the self by the self, the government of families, the government of children and so on" (295); it is often the case that hard technologies work in conjunction with or *as an extension of* technologies of governance (such as CCTV, traffic lights, building architecture, etcetera). In order to preserve circulations and/or maximize their productivity, security apparatuses – especially those which are the most complex (most often large spatial orders which accommodate large crowds and are subject to multiple spheres of governance, such as airports) - must ceaselessly respond to, adapt to, experiment with, and in some cases *integrate*, a myriad of technological advancements in order to minimize persisting risky elements, combat new risky elements, and/or maximize overall efficiency (objectives which often overlap). Identification - as well as the face - are examples of such technologies.

This project is most interested in the articulation of identity as identification – that is, identity translated as a material object which can be seen and read for the purpose of security and capital accumulation (consumerism). It is important to note that the preceding argument is *not* to suggest that identification practices are absolute in capturing and coding an individual's self-identity, or that Western subjects do not have the ability to express themselves in ways that challenge social norms and the status quo.

Pacification, if we remember, is always an incomplete (and ongoing) project that presupposes resistance, dissent and disorder. Official identity – as a pacification project - is about *fabricating* a specific type of order, namely a material identity that can be subject to the security projects of liberal capitalism. This is identification. Identification does not 'equal' identity, nor does it *determine* the self. As a contribution to pacification theory and the anti-security literature, it can be concluded from this chapter that *identification* (not identity) *is pacification* because it translates and compresses the human condition into something which can be subject to police powers and reduces personal and political expression to categories which can only be articulated through their relationship to security and circulations of capital. Therefore, facial technologies often operate an extension of this process, as the face – as a conveyer of meaning that saturates dominant culture - provides an efficient and accessible way to translate the human body for the gaze of the observer (for both humans and machines). Symbolizing the liberal subject's bondage to the database, the face functions as a truth-telling mechanism, so that the body can be subject to the security apparatus, or target marketing. The following chapter (3.2) locates identity in the discourse of surveillance, connecting these objects to social control in the post-industrial era.

3.2 What has Changed?: Identification and Surveillance Studies

> . . .the solidity of the body dissolves in data particles, detached from the whole and subject to instant reassembly as profiled and projected parodies of the person whose bodies revealed or released the data in the first place. . .the sting, of course, is that the reassembled bits are consequential, for choices and life chances (Lyon 2010: 331).

While the anti-security literature helps us to understand the productive role of the body in reproducing inequalities, as well as provides us with a political maneuver to challenge liberal allegories such as privacy; it is necessary to delve into surveillance literature and conceptualize identification under contemporary surveillance regimes. It is necessary because identification cannot be divorced from practices of surveillance.

Surveillance is central in the construction of liberal identification as such processes involve the constant intake of information - the state itself, for example, can be described as an 'intelligence-gathering machine' under which accumulated knowledge is used to help form and give shape to the social body (Neocleous 2003: 49, 50). Surveillance, as a technology of governance, has undergone a significant transformation throughout late-modernity, as security apparatuses have had to respond to the chaos of pervasive visibility through new digital technologies and the escalating transparency of the fragmented subject; such developments have jeopardized the historically 'orderly' – or *solid* - character of identification practices for Western states and institutions alike - but at the same time, have produced extensive new relationships of power which have been absorbed by networks of social control. The following section explores these issues and locates the pacification of identity in contemporary surveillance literature. By doing this we can realize a materialist conception of the body (through the face,) and push

forward a theory of facial identification as a mechanism of social control through pacification.

Anthony Giddens – writing almost thirty years ago - argues that surveillance, in whatever form, has *always* been a fundamental aspect of social organization, and that in nation-states it has reached a stage quite unmatched in previous social orders (Giddens 1985: 312); one could perhaps, make a similar claim about the state of surveillance before and after the digital revolution of the last twenty years. The technological advancements of late-modernity have presented a number of challenges to theorizing surveillance, as the ceaseless introduction and proliferation of intricate new technologies often complicates the ways in which scholars - and especially citizens - understand surveillance and its role as a technology of governance; for example, what has been increasingly difficult to determine throughout the so-called 'information era' is what processes *do not* 'count' as surveillance techniques. David Lyon and Zygmunt Bauman (2013) have overcome some of these complications with their theory of 'liquid surveillance', and drawing from that line of thought, in conjunction with ideas from scholars such as Andrejevic (2007), Lianos (2012), and Bogard (1996), this section firstly, outlines contemporary practices of surveillance and discusses its relationship to social control in late modernity. Secondly, it locates facial identification in this literature and provides a framework through which the technology can be discussed politically.

Foucault's classic analysis of Bentham's panopticon is the *arch-metaphor of modern power* (Lyon 2013), a disciplinary force which can be seen as the centerpiece of modernity (Bauman & Lyon 2013: 11). However, the longevity of Foucault's model has come into question with advent of the popularly-termed 'information era', or the 'digital

age', as the role of surveillance in the production of 'docile bodies' has arguably been overwhelmed by the advent of digital technologies through which 'power that can move with the speed of an electric signal' (Bauman & Lyon 2013: 12). The proliferation and increasing sophistication of information communication technologies (ICTs) have had a momentous impact upon the Western world and social interaction, in some cases *reinventing* certain relationships of power. These ongoing developments have called for an updated scholarly response to surveillance theory and its relationship to liberal governance. As such, scholars over the last decade have been rethinking the role of the panopticon in Western surveillance discourse, with some suggesting that we retire the theory (see Haggerty 2006), and others arguing that the panopticon is 'alive and well', and should be understood as *electronically enhanced* through digital culture (Bauman 2013 in Lyon & Bauman 2013: 55; see also Willcocks 2006: 275). While this thesis adopts the latter position, it is important to note that there appears to be a general consensus among the most prominent surveillance scholars that contemporary surveillance regimes must be understood through a *post-Foucauldian* framework. This is because, while we can still retain a semblance of the panopticon metaphor, contemporary surveillance is not only a technology of governance used to discipline populations and foster homogeneity (as Foucault famously suggested), but is *also* utilized as a mechanism of separation and exclusion within circulations of capital; as Lyon (2013) puts it: "social sorting is primarily what today's surveillance achieves, for better or for worse" (Bauman & Lyon 2013: 13).

The production of social order has undergone drastic changes following the information era, and the 'globalization' of surveillance must be framed under the larger

development of what Garland (2001) terms the 'culture of control' (Lyon 2010: 327). Having been subject to these processes, old – and previously solid – institutions, from criminal justice and marketing, to banking and borders, have *softened*, "becoming malleable and rapidly adaptive in a world of software and networks" (Lyon 2010: 325). Concrete relationships, labels and categories characteristic of the traditional regimes of social order through which control was based on the 'highly symmetric' relationship between the 'watchers-and-the-watched', have become dissolved in the chaotic free-flow of data; additionally, liberal subjects are so groomed to the role of self-watchers as to render redundant the watchtowers in the Bentham/Foucault scheme (Bauman 2013: 59, see also 57, 58). The risk management-style of governance generated by the instabilities of neoliberal capitalism - in conjunction with the consumerist turn - leaves everyone vulnerable to targeting and sorting (Lyon 2010: 331) as late-modernity casts its subjects into "…freedom of unprecedented proportions - but at the price of similarly unprecedented insecurity" (Bauman 2001: 159):

> . . .no jobs are guaranteed, no positions are foolproof, no skills are of lasting utility; experience and know-how turn into liabilities as soon as they become assets, while seductive careers all too often prove to be suicide tracks (Bauman 2001: 86).
>
> . . .anyone joining the Ford or Renault factories could have counted on staying there till the end of their working life…while people who get their lucrative jobs in Bill Gate's enterprises have not the slightest idea where they will be next year (Cohen, no citation, in Bauman 2001: 75).

The above passages, written over ten years ago, still ring true today as countless Westerners continue to suffer the consequences of systemic instability and structural inadequacies; risk-conscious culture encourages individuals to 'imagine everything that

can go wrong' and subsequently, to be 'resilient' against the brunt of any potential social problem, whether it be financial issues, job stability, or something health-related (see Neocleous 2013). The everyday disorder of individual lives is inconsequential for the order of individual institutions and the over-arching structures through which they operate; additionally, much of the anti-security literature has illustrated how insecurity functions as the primary selling-point for the marketing of security.

To locate this in the culture of individualism Lyon (2010) invokes Bauman's argument that the advertised solution in this atmosphere is '*trust nobody*' (see chapter 4.5):

> Evil lurks on every hand, and no one can be too careful. Every stranger equals danger. They could be pedophiles; they might be terrorists. Or else the other is a competitor, and again, cannot really be trusted (Bauman 2001: 331).

What should be evident here is that surveillance logic – self surveillance and the surveillance of others – is written into the very fabric of social interaction; this is but one facet through which surveillance has extended itself into the present. As Lyon (2013) argues, contemporary surveillance 'spills out all over' (3): "it not only creeps and seeps, it also flows. It is on the move, globally and locally" (Lyon 2010: 330). These 'liquid' characteristics are of course, the reason why Lyon (2010, 2013) and Bauman (2013) apply this term to describe contemporary regimes of surveillance. Most importantly for this essay, is how the solidity of identity and the body has become dissolved and fragmented by data flows - and this theme is a central feature of liquid surveillance; as Lyon delineates:

> The concept of liquid surveillance captures the reduction of the body to data and the creation of data-doubles on which life-chances and choices hang *more significantly than our real lives and the stories we tell about them* (Lyon 2010: 325, italics added).

While this passage is useful in grasping *a* core feature of contemporary surveillance (and a central theme of this essay), to summarize liquid surveillance in this way is somewhat problematic and can use some clarification. This essay illustrates that a primary task of state surveillance (and really, most - if not all - forms of surveillance) is to translate human data (both exteriority and interiority) in a way that is functional for a given circulation (through which disciplinary power can be exercised). As such, to say that liquid surveillance is interested in the 'reduction of the body to data' does not convey a new phenomenon unique to the present; one can easily point to mid-19th century photo identification as an example of how the body is reduced to data. Secondly, the concept of 'data-doubles' is equally problematic as to use the same example, the inscribing of one's identity and body upon a plastic card is no less a 'data-double' than a Facebook profile, both of which are (arguably) equally 'more significant than our real lives and the stories we tell about them'. Despite these issues, 'liquid surveillance' is a lucrative new pool of thought from which to frame the Western subject and their relationship to social control.

Themes from liquid surveillance that *are* theoretically useful here – in addition to its aforementioned pervasive, chaotic, or 'liquid' nature - is its role in social sorting and exclusion, and secondly, its relationship to the new transparency and visibility of the Western subject (and the consumer culture through which this development is engulfed). These characteristics are what make liquid surveillance "above all, *post-panoptical*" (Lyon 2013: 11, italics in original). Importantly, this theory provides an efficient

backdrop through which surveillance can be framed in the 'new social control' of post-industrialism, as the following explains.

For Lianos (2012), the socio-cultural upheaval over the course of late-modernity has led to a reworking of social order and its governing practices, which has spun advanced capitalist societies into an institutional web where 'consumption, management and administration are everywhere'. Lianos (2012) terms this present era as 'post-industrialism', pointing firstly to the dissolving of the human body into flows of data through which, according to Lianos: the body has "lost the physical importance that it had in industrial production" (a point that is addressed shortly); and secondly, Lianos places emphasis on the monopoly of institutional control over nearly every facet of social interaction, through which the agency of the post-industrial individual is always governed by an apparatus of security - to remove oneself from these apparatuses is be removed from 'legitimized' circulations of capital, dominant culture, etcetera. As Lianos (2012) elaborates:

> Normativity is identified with an extreme sensitivity to disruptions in institutional control and with the strategic preparation that such sensitivity induces. Collaboration in everyday life with the services, schemes and systems that are allied to this demand for security and the greatest possible distance from those who seem different enough to be a threat, are the two main poles of post-industrial normativity (Lianos 2012: 11).

These features of the post-industrial era are at the core of that which Lianos (2012) theorizes as the 'new social control', an approach to conceptualizing contemporary governance and relations of power that encompasses many of the themes of this essay. For Lianos (2012, 2010), social control is no longer structured around the state, but

rather, is exercised through the institutional web where the 'logic of the capitalist market prevails' (Lianos 2010: 80). The new social control operates on three axes: privatization, dangerization, and periopticity. To summarize these points, 'privatization' refers to here – broadly - the territorial dominance of institutional spaces, environments and networks; 'dangerization' refers to risk management systems and demands for security that govern institutional modes of control and classifications of inclusion/exclusion, as well the as governance of the self through which risk is managed at an individual level; and lastly, 'periopticity' refers to how institutional control transcends surveillance and disciplinary power through which "subjects are normalized by the growing refinement of the skills that seem useful to them" (Lianos 2012: 18). In other words, 'peroptic control' means that institutions become at once a socializing force that *de*socializes norms – the 'content of social existence' is so regularized such that individuals must exist and act by "conforming independently and intelligently to the multitude of institutional poles" (19).

While this type of control "perfectly exemplifies Foucault's conception of power" (Lianos 2010: 81) Lianos' analysis of surveillance as a technology of governance is necessarily post-Foucauldian (Lianos 2012: 10) as surveillance has become permanent, inverted and interactive, rendering "the panoptic prototype of a single, centralized mode of surveillance. . .obsolete and ineffective" (17, 92, 93). That being said, while Lianos (2012) locates the 'permanent gaze' of post-industrial surveillance as the core of institutional security-governance (92), his theory of 'new social control' does not need to forego the concept of panopticism altogether - there are many parallels between Lianos' perspective and the notion of liquid surveillance proposed by Bauman and Lyon (2013). However, a central reason that a more flexible formulation of surveillance is needed here

is because while Lianos' (2012) interpretation certainly acknowledges the interactive side of post-industrial surveillance, this perception is too absolute in its interpretation of the institutional subject and overlooks the increasingly active role that consumers play in contemporary consumption practices and experiences. In Lianos' (2012) words: "It is indeed another novelty of post-industrial society that it is increasingly less reliant on the input of human capacities to achieve its aims" (92). However, the escalating popularity and practice of 'custom' or 'target' advertising through which subjects are active contributors, is a form of governance that calls into question this part of Lianos' argument. One notable study on this phenomenon is Andrejevic's (2007) text *iSpy: Surveillance and Power in the Interactive Era*, which explores how interactive culture commodifies consumer-subject information for the purpose of target marketing. As such, while one may blend into the conformity of the crowd, their information – extracted from their practices as consumers - renders them simultaneously identifiable, unique, and potentially subject to individualized forms of micro-level governance, something which escapes some of Lianos' more absolute arguments. In adopting a more flexible interpretation of surveillance we can begin to interrogate the increasingly "fine-grained forms of social sorting, customization, and [information gathering]" (94) characteristic of the present.

To conclude this section, these theories of identification and surveillance help us conceptualize the face as the corporeal nexus of coded human behaviour, a function which bridges the information database with the human body. This taken for granted relationship is what makes the face a tool of pacification, as this body part has become colonized by its relationship to the material gaze of security. The following analysis

traces the history of this relationship, illustrating some of the main consequences of the face's bondage to identification. This chapter also explores some of the key ways in which identification practices become internalized by Western subjects (see chapters 4.4 and 4.5).

Chapter 4: A History of Facial Identification

4.0 Introduction

> Genealogy's task, Foucault proclaims, 'is to expose the body totally imprinted by history and the processes of history's destruction of the body (Foucault 1984: 63, cited in Hall 1995: 11).

The preceding has provided a basic theoretical backdrop from which identity and the face can be framed as a technology of governance in the form of facial identification. The following chapter (4.1) dismantles the taken for granted logic of the face as a body part which can be isolated from the rest of the human body; subsequently, I challenge some of the claims of psychological and biosocial literature, discourses which often place emphasis on the 'seeing' and recognition of faces as biological or primal. Drawing from the ideas of Delueze and Guatarri (1980), I argue that the face is a social production and that its isolation - as its 'own' body part - began to draw its visual authority from early depictions of the face of Christ, ushering in an early form of semiotic imperialism through Christian identity.

4.1 Why the Face?: Seeing, Isolating and Imposing the Human Face

> 'Primitives' may have the most human of heads, the most beautiful and most spiritual, but they have no face and need none (Deleuze & Guatarri 1987: 176).

As mentioned in the previous chapter (3.1), discussions of seeing and recognizing faces have been largely restricted to psychological literature. Much of this literature is interested in how faces are perceived – and particularly if there are notable biases in such perceptions (such as facial attraction). For example, a significant portion of this work has been focused on face perception in infants, in order to determine if humans are born with face-sensitive preferences; in other words, an 'innate knowledge' of faces. This theory was discredited in 1991 as a number of studies found that newborns could *not* discriminate between static human faces and other stimuli; however, recent research has claimed a more 'middle-ground' view as psychologists and neuroscientists have gained a better understanding of infant vision and how they visualize objects. Subsequently, face-perception studies on infants over the last decade suggest that newborns *are* more attracted to facial imagery than other environmental stimuli; discriminating between faces however, continues to be subject to much debate. For example, in a study of face-perception by one of the most prominent researchers in this field, Johnson (2011) found the following:

> A most preferred stimulus for a newborn would involve an up-down asymmetrical pattern with more elements or features in the upper half, but only when it is within a congruently shaped bounded object, such as an oval (Johnson 2011: 6).

Face perception studies on adults have also yielded some interesting results. For example, research has found that human facial attractiveness generally involves 1) symmetrical faces, 2) average faces, and/or 3) faces with exaggerated secondary sexual characteristics (such as emphasized masculine/feminine features) (Penton-Voak & Perrett 2001: 220). The role of symmetry in facial attraction has been the most consistent feature among this research as it is perceived to advertise developmental stability and health (Fink, Neave, Manning, Grammer 2006; Jones, Little, Burt, Perrett 2004). Furthermore, facial attractiveness (constructed in this way) has been found to influence court decisions, with more attractive individuals facing lighter sentences than the 'average' person for the same charges (see Kulka & Kessler 1978; Penton-Voak & Perrett 2001; Abel & Watters 2005; Berry & Zebrowitz-McArthur 2014). In addition to this, facial features associated with stereotypical personality judgements have also been a determining factor in sentencing practices, particularly for 'baby-faced' individuals (characterized by smaller chins, higher eyebrows and larger eyes - feminine features), versus 'mature-faced' individuals (characterized by more masculine features such as a large jaw and prominent brow ridge). It has been found that baby-faced adults are perceived as more honest, cooperative and sincere, but at the same time more naïve and less physically strong (Penton-Voak & Perrett 2001: 234). Subsequently, baby-faced individuals have been found less often guilty of being charged with intentional criminal behavior and receive less severe sentences for negligent crime (presumably evoking the stereotype that "they couldn't help it"), in contrast to 'mature-faced' persons who are perceived to be of equal age and attractiveness (Berry & Zebrowitz-McArthur 2014). The distinction between feminized faces and masculinized faces have also shown to have a noticeable impact on social

interaction for males as it is argued that these features contain 'stereotypical cues to personality' (Penton-Voak & Perrett 2001: 236). For example, mature-faced male teenagers tend to copulate earlier than their peers, but it is suggested that women's sexual selection leans toward baby-faced men, as slightly feminized features in males tend to signify the aforementioned 'positive' personality traits (personality traits are reportedly the most important factor in mate choice by both sexes) (Penton-Voak & Perrett 2001: 236). Additionally, research has also shown leniency bias toward smiling defendants (see Abel & Watters 2005); smiles have also been shown to stimulate infant facial perception (Faronni et al. 2007).

While this analysis is not interested in questioning the findings of the above projects, the emphasis upon the biological or evolutionary basis of perceiving human faces and discriminating between them - particularly for adults - must be subject to debate and discussion; as there is much that remains to be said about the social dimension(s) of seeing faces. This is not to reject completely the idea that discerning faces is a primal feature of the human condition, but rather, I argue that much of how we see and interpret faces – particularly in its relationship to identity – is subject to socio-cultural processes. Some studies, for example, place far too much emphasis on biological traits and take for granted the social world to which the face is situated. One face-perception study showed that individuals make the presumption that masculine-faced leaders will behave competitively in intergroup relations, and (to a much lesser extent,) feminine-faced leaders behave cooperatively (Spisak, Homan, Grabo, Vugt 2011). The authors here suggest that facial cues signify a certain biological dimension of leadership, and they create a dichotomy between 'prosocial (peace) leaders' who "focus on

maintaining and creating positive intergroup relations based on empathy, altruism, and reciprocity for beneficial cooperation between-groups"; and 'dominant (war) leaders' who focus on maintaining and creating advantage over a competing group based on dominance, risk-taking, status seeking, and so on for the overall benefit of the in-group" (2). Spisak et al. (2011) argue that the human face provided our ancestors – and still does today – with diagnostic information about 'who to follow' in adapting to conflict, suggesting that today we tend to elect masculine-faced leaders in 'times of war' and more feminine-faced leaders in 'times of peace'. While there is nothing wrong with suggesting a relationship between *assumptions* regarding leadership and feminine/masculine facial features, it becomes problematic when Spisak et al. (2011) connect this relationship to a purely statist narrative of the war/peace dichotomy, generalize the rationality and intention of 'leaders' (and make an absolutist 'evolutionary' argument that such leaders are necessary), and neglect masculinity and femininity's relationship to the social world. This chapter introduces facial perception (termed by Deleuze and Guatarri as 'faciality') from a critical realist perspective, emphasizing its relationship to culture and the social world.

Deleuze and Guatarri (1987) posit that there is something *inhuman* about the face (181); not in its physicality of course, but in the semiotic and epistemological sense. The various socio-cultural processes through which we have come to understand and organize human anatomy – to which the body is constituted as a landscape of meaning – must have, at some point in history, seen a shift from the 'body-head system' to the 'face system' that is, the emergence of a dominant discourse where the human body and its subjectivities are decoded and enveloped in the *social production of the face*. For them,

the human face is a politics (Deleuze & Guatarri 1987: 181); it is a historical invention and an imperial force. The notion of a 'face' represents both a 'deterritorialization' and a 'reterritorialization' of the human body (a sort-of creative destruction), as the face "removes the head from the stratum of the organism, human or animal, and connects it to other strata, such as signi-fiance [sic] and subjectification" (Deleuze & Guatarri 1987: 172). Thus, the 'inhumanity' of the face lies in its cultural over-coding and absorption of bodily subjectivities (including clothing); in short, the face functions as the corporeal centerpiece of human expression – a 'black hole' of subjectivity as Deleuze and Guatarri put it. And while 'seeing' a face involves a degree visual classification and ordering, – a process described as '*faciality*', - the social production the face is certainly not a product of the Enlightenment or early-modernism, as what can be described as 'facial discourse' has been unfolding throughout history. For example, Deleuze and Guatarri (1987) posit a major turning point of this epistemological movement in Christianity and the face of Christ. The figure of Jesus, as the physical manifestation of God, both divine and human, influenced the discourse of Christian identity and its relationship to the body, which began to assign authority to the face as a truth-telling mechanism through which human beings became *subject* to their facial traits. This movement sparked the imperialist dimension of 'facialization', through which the face is organized and *imposed* upon humanity. In this instance, the face became deployed through Christian ideology as a 'semiotic imperialism' – absorbing language and discourse – especially that of identity and the body – into an 'ideal' faciality.

Since faciality is politically and aesthetically oriented, the face shares the qualities of a *landscape.* In the same way that geographical borders and territories are established

through the logic of sovereignty, faces can be similarly described as 'fabricated spatial orders' which are established and given meaning (Neocleous 2003: 124). And just like mapmaking was a means of imagining a history and a future for a rendered landscape (Bantjes 2003: 16), the very idea of the face suggests a way in which facial features 'ought to be' appropriated. Interestingly, Deleuze and Guatarri suggest that the inception of Christian facial discourse – through imagining the 'borders' of the face and locating the ideal in Christ - began to form the bedrock for racist ideology:

> If the face is in fact Christ, in other words, your average White Man, then the first deviances, the first divergence-types, are racial: yellow man, black man, men in the second or third category. . . They must be Christianized, in other words, facialized . . . Racism operates by the determination of degrees of deviance in relation to the White-Man face, which endeavors to integrate nonconforming traits into increasingly eccentric and backwards waves, sometimes tolerating them at given places under given conditions, in a given ghetto, sometimes erasing them from the wall, which never abides alterity. . . (Deleuze & Guatarri 1987: 178).

Additionally, not only did the normative face (of Christ) potentially trigger the ideological underpinnings of 'race', but it also influenced understandings of social *belonging* and its relationship to the body – the 'backdrops' to which faces may fall – or perhaps more accurately, where it was believed they 'should' fall. This can again be linked to the logic of 'landscapes' and spatial order, as 'bodily-aesthetic spaces within geographically-aesthetic spaces' – in other words, the authority of Christ's face arguably provoked the long-standing belief that *certain faces belong in certain places* – ie.: that facial types 'belong' to certain nations, that certain facial features 'belong' to each sex, or that certain faces do *not* belong in certain positions of authority. This type of logic may have informed discourses where the biological uniqueness of women, like skin color and

facial characteristics for African Americans, became a basis for treating them as inferiors (Zinn 2005: 94). While more research needs to be conducted on the earlier histories of face-perception and its social implications, it was not long until facial discourse became engulfed in ideologies of 'race' – especially, but also of sex and class (as we will see); ideologies which eventually became scientized in the mid-19th century and institutionalized through American eugenics programs and the horrors of 20th century fascism. Cesare Lombroso is one of the most significant figures in this history, as his ideas regarding the 'born criminal' were particularly influential in the establishment of eugenics programs and in augmenting the bio-criminology of Nazi scientists (Lombroso's works were translated into German toward the end of the 19th century) (see Rafter 2008; Ferguson 2007).

Racism's relationship to the face is a historically significant one, as facial features became a paramount object of study for those who pioneered scientific racism; Cesare Lombroso, an Italian criminologist writing in the late nineteenth century, is perhaps the most famous of these individuals, as his theories of crime - drawing heavily from psychiatry and the logic of Social Darwinism - were particularly influential in the eugenics movements of the early twentieth century. Lombroso (2006; orig. 1876) argued that criminals are born with 'evil inclinations' (48); for him, criminality is innate in the biology of the individual and can be 'empirically' read from the body. While Lombroso focused on just about all aspects of the visible human body to develop these theories (such as hands, height, weight, even handwriting, artistic ability and tattoos), the face was a significant part of his analysis. While Lombroso went to the extreme of robbing graves to locate body parts upon which to test his theories (Walby & Carrier 2010), he also

relied on the technology of photography. With cameras becoming a tool of criminal investigation in the late nineteenth century (allowing police to identify repeat offenders), colleagues from around the world sent Lombroso photographs of convicted criminals, from which he claimed he could locate criminality among the depicted persons' physiology (Gibson & Rafter 2006: 203). The findings of this logic is outlined in the following passages:

> Nearly all criminals have jug ears, thick hair, thin beards, pronounced sinuses, protruding chins, and broad cheekbones (Lombroso 2006; orig. 1867: 53).
>
> Habitual murderers have a cold, glassy stare and eyes that are sometimes bloodshot and filmy; the nose is often hawklike and always large; the jaw is strong, the cheekbones broad; and their hair is dark, abundant and crisply textured. Their beards are scanty, their canine teeth very developed, and their lips thin. Often their faces contract, exposing teeth (Lombroso 2006; orig. 1876: 51).

While the bulk of Lombroso's criminology tended to focus on the criminality of males, Lombroso (2006; orig. 1876) did write rather extensively on women, positing that female criminality is characterized by an 'exaggerated sexual drive' (as prostitution) and secondly, that masculine features characterize the faces of female criminals of all nationalities; in his own words: "Like prostitution, criminality is increasing among women with the progress of civilization, which makes them more like men" (128). These theories also extended into the realm of class, where Lombroso posited that the rich can better resist criminal impulses because they are "physically and morally fortified by sufficient nutrition and good education"; on the other hand, Lombroso argued that wealth "can also cause degeneration (from syphilis and orgies)" (322). Lombroso's most influential statements however, came from the connection of this logic to issues of 'race';

positing that racialized features were a biological determinant of atavistic behaviour, and in the case of crime, violence and cruelty as well (19):

> Those who have read this far should now be persuaded that criminals resemble savages and the colored races. These three groups have many characteristics in common, including thinness of body hair. . .small cranial capacities, sloping foreheads, and swollen sinuses. Members of both groups frequently have sutures of the central brow ridge, precocious synostes or disarticulation of the frontal bones, upwardly arching temporal bones, sutural simplicity, thick skulls, overdeveloped jaws and cheekbones, oblique eyes, dark skin, thick and curly hair, and jug ears (Lombroso 1876: 91).
>
> In studying crime among savages, our earliest human ancestors, we face the same difficulties that we encountered in the animal kingdom. Here, as with animals, crime is not the exception but almost a general rule. This is why so few have understood the behaviour of savages to be criminal or recognized in it the origin of modern criminality (Lombroso 1876: 175).

Perhaps unsurprisingly, Lombroso – having Jewish ancestry - refused to characterize Jewish behaviour in simple biological terms and turned to more complex sociological explanations. He argued that Jewish patterns of behaviour derived from the historical legacy of persecution rather than from innate racial characteristics (Gibson & Rafter 2006: 18): "[the Jews] were often merely shuttlecocks between the armed brigands and the feudal lords, and were forced to be accomplices in order not to become victims" (Lombroso 1911: 39; see also Lombroso 2006; orig. 1876: 118, 119)).

Psychiatrists writing on 'moral insanity' at the time made very similar postulations regarding faciality and 'undesirable behaviour', as the medicalization of moral transgressions (namely, anything believed to transgress the limits of (Anglophone) bourgeois civility and morality (Rimke 2003: 257)) became intertwined with assumptions about 'race', class and gender. Outstretched ears, and asymmetries of the face were

criteria for establishing moral insanity (Rimke 2003: 251) and psychiatrists such as Benjamin Rush (1839) argued that faces which "resemble each other, have same manners and dispositions" (20). Subsequently, drawing from Social Darwinism and evolutionary laws (yet underpinned by a Christian morality), these medical texts argued that 'dark-skinned races' were categorically disqualified from possessing a moral faculty, and that the 'superior races' risked 'race-degeneracy' should they not tame the "animal appetite" characteristic of 'primitives' (Maudsley 1868). Physical measurements against the 'average white man' were said to be 'proof' of the innate inferiority of non-white races – those bodies perceived to deviate most from the 'ideal type' became pathologized or racially inferiorized.

Like Lombroso's theories of criminality, this logic played into gender and class as well. While faciality was certainly not the only corporeal form of measurement of moral pathology, subjects' faces were scrutinized and measured against bourgeois social standards of normative masculinity and femininity (Rimke 2003: 255). Morally insane men, for example, were described as having more feminine facial features; and by contrast, morally insane women 'defeminized' features (Connelly 1858: 651). And in regards to class, subjects of 'lower origins' were described as having a 'filthy', 'unruly' and 'disorderly' look. Connelly (1858) describes one morally insane poor person as follows:

> Here the bloated face, that pendulous masses of cheek, the large lips uncontrolled by any voluntary expression, and to which refinement and delicacy seem never to have belonged; that heavily gazing eyes, not speculative, scarcely conscious; the disordered, uncombed, capriciously cut hair, cut with ancient scissors or chopped with impatient knife. . . (Connelly 1858: 651)

By contrast, inherent in the interpretation of an 'upstanding' moral person, was evidence of a healthy and well-nourished physique. Bucknill & Tuke (1858), for example, argued that "good nature usually coexists with a sleek and fat habit of the body". This is not to say that members of the bourgeois were *not* subject to the diagnosis of moral insanity, but quite the contrary; the origin of moral insanity offered for the middle and upper class routinely removed responsibility from them for their pathology, whereas the poor were perceived to be naturally predisposed to moral madness (Rimke 2003: 254). The fact that members of the upper and middle-classes were potential candidates for moral degeneration "represented and demonstrated a bourgeois fear of becoming like the 'Other'" (Rimke 2003: 254).

Considering the glaring parallels in these lines of thought, it is unsurprising that Lombroso (2006; orig. 1876) draws from the medical literature on moral insanity in some of his work. In perhaps the most interesting case, Lombroso, unable to find any consistent "signs of physical degeneration", pinpointed the criminality of political criminals and revolutionaries in the discourse of moral insanity, arguing that their criminality is related to their 'moral imbalance', as opposed to atavism (286) (Lombroso analyzed their photographs as well). Reinforced by the authority of other scientific discourses such as the proponents of moral insanity, Lombroso's arguments corresponded with the political climate of the time and along with other like-minded scholars, these ideologies injected racism into the new field of criminology and broader scientific and social thought. Eventually, the deterministic ideas in *Criminal Man* and the concept of moral insanity expanded into a more general concern with the organizing concept of 'degeneracy', which broadened into the new master discourse of 'eugenics' (Rimke & Hunt 2002).

While the face was a small part of this movement, the 'pathologizing gaze' (Walby & Carrier 2001: 263) pioneered by figures like Lombroso dominated the visual interpretations of bodies and their relationship to the social world until the advent of World War II. Castel outlines this turning point quite effectively in the following passage:

> . . .the monstrously grotesque version provided by Nazism helped both morally and politically to discredit eugenic techniques which, but for this tragic episode, would doubtless have has a fine future ahead of them" (Castel 1991: 286).

While racist, sexist and classist ways of seeing the face have certainly not disappeared, the discrediting of scientific racism following World War II shifted the trajectory of facial discourse and its relationship to these variables, particularly 'race'. Dominant forms of racism began to distance itself from theories of biological determinism and became recast into the inferiorizing of cultural/ethnic representations – referred to by some scholars as 'new racism'. It is the case now for example, that faces of any 'color' or sex can command authority as a talking head of television news networks – so long as they reflect the dominant (white) culture's gender norms, fashion style, accent, language, appearance, politics, obedience and are of a 'respectable' age. To use another example, US army uniform and appearance regulations recently banned most twists, dreadlocks and large cornrows as not displaying a "neat, professional, well-groomed appearance"; these regulations obviously single out the ethnic appearance of African American women (Department of Army 2014: 6). Thus, even though the crude racism of the past has become 'officially' divorced from institutional narratives of interpreting faciality and the body, *discrimination* based on racial ideas has certainly not been

interrupted by these processes, but rather, has adapted to the rationalities of the institutional world, a world that relies on the racial, gender, and economic inequalities that define the status quo. This thesis shows how facial identification has been an important part of rationalizing discrimination in the twentieth and twenty-first centuries.

The preceding has illustrated that the face - as perhaps the most taken for granted product of discourses on the body- is *not* a universal. It should be evident that Deleuze and Guatarri (1987) adhere to this argument (see 176) and more recently, scholars such as Gates (2011) and Haraway (1998) have posited this as well, asserting that there is no universal way of 'seeing' the face because it is caught within the constant struggle over visual sovereignty (Gates 2011: 9, 11); thus, it can be said that what 'counts' as rational accounts of the world are struggles over *how* to see (Haraway 1998: 681, 682). While facial discourse is historically and socially contingent, the dominant meanings that become attached to faciality – how we see the presumed face – continues to carry a largely uncontested authority; and as we begin to dismantle facialization by acknowledging these socio-political and historical conditions to which faces materialize, this begins to uncover certain relationships of power; that is, the extent to which our lives are conducted by - and through - the visual authority of faces:

> Choices are guided by faces, elements are organized around faces: a common grammar is never separable from a facial education. The face is a veritable megaphone (Deleuze & Guatarri 1987: 179).

As later sections explore in more detail, one need only turn on the television or open a magazine to see the ways in which faces absorb culture, project knowledge and command authority. Magazines and advertisements emit masculine and feminine ideals of faciality,

the trusted faces of news anchors project knowledge and expertise, the familiarity of famous faces are used to sell products, and 'dangerous' faces are used to sell newspapers and war - various media outlets for example, featured images of Osama Bin Laden describing him as the 'face of terror' (see CNN Wire Staff 2011; Star Wire Services 2011; Zernike & Kaufman 2011; Daily Mail Reporter 2011). These simple examples illustrate the ways in which the face has become instrumentalized throughout the 20th century – employed as a technology of governance; the largest employer of faciality being of course, the modern state-surveillance complex. The following section explores the marriage of faciality to liberal identity and citizenship in the early 'securitization' of facial discourse in the 19th and 20th centuries.

4.2 Seizing the Body through Photography

> Visibility is a trap (Foucault 1995: 200).
>
> Basically all technology is made for ordering the world and reproducing it. Modernity has applied these ordering techniques to humans, under the general category of discipline. It has produced its own masterpiece: the rational subject biographically, socially and politically modern (Lianos & Douglas 2000: 263).

It should be evident from the preceding section that the face occupies a unique position of visual supremacy quite unmatched by other signifiers of the human body. The face is the 'signification of the self in relation to others' (101), the unique architecture and immediacy of the face speaks a degree of 'truth' which other bodily features do not. In modern discourse, seeing the face provides us with an immediate – if rather crude -

knowledge of the other, such as their approximate age, gender, ethnicity, perhaps their current emotional state and health (ie: she 'looks' sick, he 'looks' angry); and importantly, it is often the most accessible way to visually differentiate between human beings – who we 'know' or who we do not know (who we can identify). This type of knowledge and its relationship to faciality is of course, saturated with dominant interpretations of identity and other various cultural meanings. While the face has always operated as a pivotal component in how individuals conduct themselves and others, its role as a visual technology has been less significant for the sovereign state until quite recently. The following sections of this historical analysis traces faciality as an instrument of the liberal state; in other words, it explores the face's role in population management through the marriage of official identity and the visualized body.

The notion of 'identity' has always operated as a paramount feature of the nation-state in its management of populations. Since the nation-state consists of a singular, unified and self-determining population (Nash 2000: 159), the liberal state is ceaseless in its effort to reduce the human body to a coded vessel, that is, "individuals who can be compared contrasted, added and subtracted from each other as abstract persons" (Neocleous 2003: 53). Thus, it can be argued that translating humans into *statistical* data is a paramount objective of the state in its effort to coordinate the social body; liberalism as such, is posed with the impossible task of capturing a singular identity from the fluid and always-shifting nature (Avery-Natale 2010: 96) of the endlessly performative self (Hall 1995). Importantly, this type of narrative continues to dominate modern interpretations of identity by Western subjects as mass culture constructs it as something

which is static, stable, and knowable - as something that can be 'captured'. As Bauman aptly puts it:

> . . .the quandary tormenting men and women at the turn of the century is not so much how to obtain the identities of their choice and how to have them recognized by people around – but *which* identity to choose and how to keep alert and vigilant so that *another* choice can be made in case the previously chosen identity is withdrawn from the market or stripped of its seductive powers (Bauman 2001: 147). . .The 'identities' sought these days are such as 'can be adopted and discarded like a change of costume' (148).

The relationship of identity to late-modern consumer culture is explored in more detail in later chapters (4.3, 5).

Faces meant little in the way of state governance prior to the modern era, as populations were often more homogenous, predictable and spatially fixed; individualized identification was not a significant social problem for governments. The nation-state maintained social control with a minimum of coercion and a maximum of law, "made palpable through the fanfare of patriotism and unity" (Zinn 2003: 99) and authorities relied heavily on words, in the form of names and physical description. Permanent patronyms were constituted politically and went far in 'helping fashion a legible and thus knowable people' (Neocleous 2003: 57). Descriptions of clothing were also useful as for example, garments were significant indicators of status in a largely socially immobile Europe (Tudge 2011: 24, 25). As Aas (2006) delineates:

> . . .in Europe there was no need for last names until the Middle Ages. . .[it was not until the 19th century] that identification of people grew increasingly difficult, due to the growing anonymity and mobility of populations, the growth of cities and immigration across the Atlantic (Aas 2006: 146).

Because the state views identity as something to be captured, it was not long until the observable body became subject to techniques of population management. It might be assumed that faciality was significant for the liberal nation-state for the most part of its history, for example, throughout the four-hundred years of American slavery – differentiating through legislation, between 'white' and 'black' faces. However, while 'seeing' faces may have been dominated by the racist perceptions of the time, it would be more accurate to say that, in regards to slavery, the state placed emphasis upon the differentiating of racialized *bodies*, discrimination which depended more on skin colour than facial traits. Thus, it is not for quite some time - until the 19th century - that facial discourse became pertinent for the purpose of security and governance; this is through the tethering of identity to the technology of photography (articulated as identification).

Visual sociologist Paglen (2011) makes the assertion that "photography is becoming more and more inseparable from the workings of state power, corporate interests, and our everyday lives" (68). This chapter illustrates that the technology of photography – specifically the camera, invented in 1826 – was *immediately* co-opted by the state for law enforcement purposes. Contrary to Paglen's argument, there was a *very* short frame of time that photography was ever separable from state power, and as such, corporate interests and everyday life. Photo identification was the first way for Western governments to coordinate a *visual* identity in order to better impose state narratives upon the physical body; and, like the introduction of most mechanisms of surveillance, facial identification began with the monitoring of social deviants. Photography was proving to be a cheap and easy way of identifying inmates (Tudge 2011: 92), a technique which eventually became imposed upon additional criminal actors – where by 1858, for

example, the NYPD "had a collection of 450 photographs of the most notorious offenders" (Garfinkel 2000). Zinn (2003) provides a unique visualization of this early process of state identification from an item in the *Boston Transcript* of 1895:

> A colored man who gives his name as Henry W. Turner was arrested last night on suspicion of being a highway robber. He was taken this morning to Black's studio, where he had his picture taken for the "Rogue's Gallery". That angered him, and he made himself as disagreeable as he possibly could. Several times along the way to the photographer's he resisted the police with all his might, and had to be clubbed (Zinn 2003: 191)

Additionally, it was also around this time – the mid 19th century - that the 'wanted poster' emerged as a common police practice, applied most vigorously in the unruly segments of the American Frontier – better known as the 'Old West'. Complex figures like William Bonney (aka Billy the Kid), the notorious outlaw who was defined solely through eye-witness accounts and tall tales - illustrates the diluted and disorderly character of individual identity at this time, and subsequently how frustrating this was for law enforcement (Jameson 2005: 64). For example, there is ongoing debate about whether William Bonney was actually killed by lawman Pat Garrett in c. 1881, as no one could confirm that the dead body belonged to the infamous fugitive. While William Bonney's face was never displayed for the purpose of public notoriety, traditional wanted posters often featured a composite sketch of the offender's face or included their photograph, with one of the earliest American posters featuring a photo of John Wilkes Booth, wanted by the War Department in 1865 for the murder of Abraham Lincoln.

It is also important to note that photography in the 1840s on onward was used to both humanize and dehumanize African Americans. Following its invention, the

scientific community saw figures like Lombroso using photographs of coloured people to 'demonstrate' their 'savagery', and this form of white supremacy extended into all facets of Western culture, now with a new device at its disposal:

> . . .photo-graphic technology [became] responsible for the circulation of minstrel caricatures, of dim-witted watermelon-eating Negroes, of alleged African cannibals, of happy-go-lucky darkies whose lives revolved around dice and razors (Willis 2000: ix).

Some white families would also take family portraits in blackface, mimicking the perceived inferiority of African Americans for a comedic effect of the time.

Racist and one-dimensional depictions of African Americans carried on well into the early-twentieth century. For example, in most product advertisements of the era "blacks [were] shown as producers (workers, cooks) or servants, or as decorative elements, but *not* as *consumers* of the product" (Pieterse 1992, italics in original). White photographers were not sensitive to the racist depictions of blacks in dominant cultural imagery, and subsequently, most African Americans sought out black photographers in order to achieve respectable depictions of themselves and their families:

> Negroes can never have impartial portraits at the hands of white artists. It seems to us next to impossible for white men to take likenesses of black men, without most grossly exaggerating their distinctive features. And the reason is obvious. Artists, like all other white persons, have developed a theory dissecting the distinctive features of Negro physiognomy (Douglass 1849 cited in Willis 2000).

Thus, while the camera functioned as a powerful extension of semiotic imperialism (in the form of white supremacy), in the hands of black photographers the technology was essential in countering the stereotyping of black society and in helping the community

reclaim their visual sovereignty (Willis 2000: 38). Hooks (1994) argues that the camera provided a means to document a reality, and was therefore the central instrument by which blacks could disprove representations of themselves created by white society.

To conclude this section, the invention of photography awarded authority to images of white supremacy and, utilized by law enforcement institutions, introduced faciality as a facet of modern liberal governance as facial features became something to be captured, recorded, authorized, registered, stored, and tracked. The technique of photo identification was so cheap and efficient that it soon became a staple of Western society and state governance more generally. With populations becoming more heterogeneous, politically divided, ethnically diverse, and altogether more disorderly, standardized identity documents - complete with photo portraits - were introduced in the early decades of the 20th century. However, there is no definitive 'origin' of these identity documents across the West. In Canada for example, passports were introduced following the demand that Indians emigrating to Canada present identification documents. Mongia (1999) argues that this was a way to disguise methods of discrimination that sought to achieve the desired ends of curtailing immigration, as this demand followed public anxieties over migration around 1906, with the arrival of about two thousand Indian men in Vancouver (533). The Canadian passport program was hugely successful, as between 1909 and 1913, only twenty-seven Indians managed to enter Canada (Mongia 1999: 541). Not long after, the static image of the face – or the portrait - became the central component for linking the human body to an increasingly sophisticated mechanism of identity construction as Western citizenship now requires that individuals surrender their faces for full and legitimate participation in society. As David Lyon (2010) puts it: "the database. . .

determines who should be included for full access to consumer privilege" (328). The widespread implementation of the information database firmly anchored the visualized face as the central corporeal gateway between state narratives of identity and the liberal subject; it was through these processes that faciality became instrumentalized as each individual's personalized key to the markets. The following section looks at how facial discourse - and its marriage to the identity database - became intertwined with the proliferation of visual surveillance technologies in the 20th century – specifically CCTV and the credit card industry.

4.3 Information Communication Technologies (ICTs) and the Financialization of Identification

With the face becoming a central feature of population management following the development of photo identification in the 1960s, Western institutions began to implement surveillance technologies that exploited this dimension of the information database. Facial identification became not only a social issue for the state, but for the commercial sector as well. Initially targeting consumers, CCTV cameras (originally used to observe test launches of V2 explosives in 1942,) began to be installed in department stores in the late 1960s, and later became integral "to the design and management of vast shopping malls that erupted worldwide from the late 1970s and 1980s atop the credit card consumer boom" (Tudge 2011: 83). Affirmed to be an effective deterrent to shoplifting and other crimes, the installation of ceiling mounted video cameras

throughout the Western world allowed the face to be 'seen' by an expanding commercial gaze, facilitating a purposeful administration of these zones in the name of security (Lyon 2010: 327) and as retailers quickly discovered - video cameras became an effective way to monitor employees as well (Lyon 2001: 13). Their presence became significant as individual identity continued to be dissolved into data particles with escalating social weight and consequences (Lyon 2010: 331), the face-database had emerged as a prime target for new mechanisms of innovative governing technologies. Perhaps most significantly, was the attachment of finances.

Around this time, in the 1980s, banking in the West became reorganized around information communication technologies (ICTs), through interconnected computer networks and electronic funds transfers (Gates 2010: 422). As an extension of the database, Westerners became represented through plastic cards electronically bonded to a constellation of devices, networks and practices, which facilitated a massive proliferation of data about their financial transactions (Gates: 422, 425). Financial records documented what people bought, as well as what they read, how they played and drank, where they vacationed and where they lived, and many other things about their everyday lives (Turow 1997 in Gates 2010: 423). The increasing social weight of financial identity also entailed a plethora of new technological security measures, as credit cards could be lost, stolen or obtained in other fraudulent ways (Gates 2010: 423). Thus, the *financial* 'securitization of identity' was set in motion. Rose (1999) defines this process as "the proliferation of sites where individuals are made responsible for establishing their official identity as a condition of access to the right and responsibilities of citizenship," (241). And while the face was touted as a 'security guard' of modern financial identity (used in

conjunction with CCTV cameras and routine ID checks to help deter fraud and identify criminals), the connection of financial data to the official photographed portrait did little to protect personal information from various financial exploits and crimes. As Whitson and Haggerty point out:

> …[identity theft protection services] are themselves part of a political strategy whereby institutions are divesting themselves of responsibility for the full social and economic costs of the risks they have produced (Whitson and Haggerty 2008).

Thus, not only was the financially inscribed identity used to monitor and conduct consumer-populations, but individual subjects were expected to manage their own identities and govern themselves according to the identities of others – financial-identity became commodified as an object of security. And despite the failure of security programs to secure against new financial insecurities, visual surveillance increasingly became a principal feature of state and commercial institutions as CCTV networks began to saturate vast segments of the Western world, serving increasingly managerial purposes (such as circumscribing risk in commercial sectors) (Rigakos 2008: 195). This securitization of financial identity was part and parcel of the 'consumerist turn', which emphasized developments in heightened individualism, insecurity (and thus the marketing of security (see Spitzer 1999)), and the surveillance of others where "trust is eroded at every turn" (Lyon 2010: 331).

It was not long, however, until state-centric identity became destabilized by the revolutionary technological developments of the information era – specifically the advent

of the Internet. Moving toward the present time, the commodification of the database exposed liberal subjects to new kinds of visibility "…making them amenable, as risks, to new kinds of governance," (Gates 2010: 424, 427). These developments spearheaded the post-disciplinary shift into what many scholars term the 'risk society' or the 'control society', where the notions of risk, insecurity, security and surveillance became very closely connected (Lyon 2010: 327, 328; see also Beck 1992, Giddens 1990). In correlation to the developments in Internet technologies, generally characterized as Web 2.0 - essentially *pure* communication (Beresford 2003: 88) - the data-mining culture of advanced liberal democracies accentuated the transparency of the liberal subject through their relationship to the database. It is the case today, for example, that information is ritually and relentlessly extracted from those who wish to participate in almost any form of citizenship or consumption (Best 2010: 8). This has lead, once again, to new disciplinary challenges to – and opportunities for - liberal identification practices (chapter 5.2 will explore this in more detail).

As Beresford (2003) puts it: "by freely exchanging knowledge, more knowledge, power, and freedom are created" (100). The sudden explosion of new avenues of digital communication (embodied in social networking, online profiles and political and religious mobilization, and broader digital transactions etcetera,) have destabilized the solid frame of state-centered identification, through which the expression of the self has begun to permeate all aspects of social life, in a variety of fragmented ways. Internet communication provides users with a degree of anonymity, detaching them from the human body (in the creation of 'data doubles' (see Lyon 2010)), thus escaping the disciplinary gaze of the state. This knowledge leakage, along with the deregulated

structure of the 'wild web', provides Western liberalism with new challenges in constituting a virtual spatial dimension of "totally useful time" (Foucault 1995: 150). The unprecedented liberty of travelling through cyberspace has yet to be colonized by state security, and the fragmented-virtual identity has fashioned a mass of new insecurities and risks, constituting fresh targets for preventative intervention (Castel 1991: 289). In the traditional disciplinary fashion, the (digital) body must be made useful and efficient, and productivity must be maximized. Legislative efforts such as the Protect IP Act (PIPA), Stop Online Piracy Act (SOPA), Anti-Counterfeiting Trade Agreement (ACTA), Bill C-8 and the North Atlantic Free Trade Agreement (NAFTA) are some of the most recent attempts by liberal states to quash online anarchy and help gravitate disorderly information highways back toward 'knowable' bodies - as an effort to (re)mobilize fragmented Western identities for state and corporate interest. The recent ruling by the US Federal Court of Appeals for the District of Columbia Circuit for example, has nullified key provisions of the Federal Communications Commission's (FCC) net neutrality rules in January 2014: "opening the door to a curated approach to internet delivery that allows broadband providers to block content or applications as they see fit" (Kravets 2014). Craig Aaron, president of Free Press – an advocacy organization devoted to promoting democracy through media technologies - paints a vivid picture of the potential consequences of this provision:

> [Under today's ruling] broadband providers will race to turn the open and vibrant Web into something that looks like cable TV. They'll establish fast lanes for the few giant companies that can afford to pay exorbitant tolls and reserve the slow lanes for everyone else (Aaron 2014 cited in Kravets 2014).

Without moving too much further into the present, it is necessary to consider some of the other socio-political consequences of identification and its relationship to order-building – specifically in relation to crime and dominant cultural productions of faciality. The following section will illustrate how many Westerners continue to internalize institutional (visual) portrayals of identity, leading in some cases to support for police projects and war efforts.

4.4 Visualizing Risk Through Contemporary Faciality: TV News and War Discourse

Televisual news, in usurping the more traditional platforms of media (such as radio and newspapers) with greater powers of validation through the broadcasting of 'real' footage, relies upon the epistemology that 'seeing is believing' (Doyle 2006: 211). However, the authority commanded by this now-common style of news production is often questionable because as Ericson (1998) points out:

> TV news has not literally shown us what it is telling us about; it has featured after-the-fact recounting of events by 'talking heads' rather than actual footage of the events in question (Ericson 1998).

Because the 'showing' of live news events is often difficult, impossible or simply not necessary for profit-oriented news outlets, constructing visual narratives through *faces* is (perhaps obviously), a central facet of visual news media.

More than ever, contemporary TV news reproduces the face's bondage to security and the state in innovative new ways, particularly in the reporting of crime news. For

example, Doyle (2006) discusses the contemporary practice of displaying 'video wanted posters' in TV news programs, as well as so-called 'reality' entertainment – referred to in some cases as 'infotainment'. The video wanted poster involves the TV audience being asked to view surveillance footage in order to help officials with investigations – quite similar in theory to the wanted posters of the past. A big difference however, – aside from the technology - lies in the cooperation by third party sources outside of the state, such as the owners of the footage (convenience stores, gas stations), and of course, the local TV news stations who broadcast the video. And importantly, there has been significant developments in the video wanted poster tactic since Doyle's account of it in 2006; the latest incarnation involves the proliferation of video recording technology through cellular phones and the like, where citizens and social media websites have also been recruited to identify police suspects. A good example of this is the Vancouver Stanley Cup riots of 2011, where hundreds of Canadians posted pictures of suspected rioters on Facebook in order to support police efforts in identifying and charging individuals involved in the destruction of property. According to the Vancouver Riot 2011 website - maintained by the Integrated Riot Investigation Team (which continues to seek help from citizens) - thousands of photos and over 5000 hours of video footage have been submitted by the public (Vancouver Riot 2011 2014) (see also section 5.1: "Local Law Enforcement and Other Applications: The Limitations of Uncontrolled Facial Recognition Software"). What is notable here is that the website's photographs of the 'most wanted' individuals contain only their faces, completely removed from the act of property destruction (imagery that previously characterized the photographs posted on Facebook).

The face's bondage to security has also disproportionally affected people of colour, those communities who are most often subject to security intervention and policing. Subsequently, the *representation* of racialized faces is dominated by security narratives, which continues to be a significant theme in contemporary news and entertainment media. Activist and poet Olivia Cole puts it quite well in the following excerpt (2014):

> As white people, we are used to representations of ourselves crowding the covers of magazines, crowning the posters of newly released films. The good guys are white, we have learned, after eons of our faces being plastered under cowboy hats and in impeccable Bond suits. White men are Superman, we have learned. White men are Ethan Hunt and Neo and white men are hobbits. Bad men, we have learned, are black. They're gang bangers and thugs and talk loud and sometimes deliver funny lines where we laugh at their Otherness. Black men aren't heroes, we learn. Our imagination and subconscious are so saturated with white supremacist notions of goodness, beauty, and heroism, that when confronted head-on with an image of a black man who is brilliant and kind and normal and who saves the day, we transform into robotic versions of ourselves: Does… not… compute. Hero… must be… white. It's this line of thinking that turned Disney's Princess Tiana into an animal for 95 percent of the movie. The collective white imagination had difficulty imagining a black girl as a princess… and so she became a frog (Cole 2014).

Additionally, the West has also seen the demonization of Muslims through one-dimensional news accounts, Hollywood films, video games, and other media platforms, as well as through the criminalization of the Muslim religion by terror legislation in the West. These processes have brought the Muslim face to the forefront of Western public discourse on terrorism and the Global War on Terror more generally.

In introducing the FBI's 'most wanted terrorist watchlist', US President George Bush stated that: "Terrorism has a face and today we expose it for the world to see" (White House 2001, cited in Gates 2010: 107). There is perhaps no category of identity as

"unruly or unstable as that of the terrorist", and the twenty-first century image of terrorism materialized largely through depictions of the Muslim religion and the faces of Arab men more generally (Gates 2011). While "the face of terror" term was never used by Bush (as adopting such a term would suggest too explicitly that terrorism has a facial type (107)), it became coined by various sects of US security discourse - particularly in discussions of the FBI's 'most wanted terrorist watchlist' and also in related efforts to implement facial recognition technology (122). Thus it can be said that the 'face of terror' serves a biopolitical function: "brandished as a weapon to justify state racism and define the war on terror as a virtuous one" (Gates 2011: 122). Additionally, giving a 'face' to terrorism reinforces the taken for granted authority of law enforcement officials and the state in their monopoly over identity, which has continued to anchor the information database as a truth-telling technology. For example, in the collection of digital wanted posters under the FBI's 'most wanted terrorists' website "there appears to be no ambiguity or uncertainty about the identities of the individuals depicted. . .visitors to the site need not question the source or factual nature of the information presented" (Gates 2011: 115). Visitors are also encouraged to 'submit a tip' (through which rewards are offered) and even *print* the wanted posters – alluding to the possibility that members of the public may 'run into' a terrorist one day (see fbi.gov 2014). The difference between the FBI's 'most wanted' list and the 'most wanted *terrorists'* list appears be little else than for the latter to stabilize the war effort by providing a 'caricatured version of the enemy', bolstered by the stereotypes exploited by the mainstream press and entertainment media. The trope of the "face of terror" - without explicitly saying as much - has invoked specific objects: "mug shots and grainy videos of Arab men" (Gates 2011: 106).

It is important to note however, that dehumanizing the face of the enemy in mobilizing public discourse (through official narratives, mass media and otherwise,) is not something new to Western warfare. As Gates (citing Keen 1986) explains:

> At least since World War II, propagandists have recognized that the "job of turning civilians into soldiers" could be achieved through the uniquely effective tactic of superimposing a variety of dehumanizing faces over the enemy "to allow him [sic] to be killed without guilt" (Keen 1986: 12).

World War II and Cold War propaganda are both demonstrative of this; where for example, political cartoonists of their respective eras would racialize the enemy by exaggerating the facial stereotypes of Japanese and Vietnamese people, emphasizing their otherness. While it could be argued that what distinguishes the War on Terror from the wars of the past in regards to facial discourse is the ambiguity of both the terrorist identity (despite government efforts to organize it) and the 'battlefield' – where the enemy is potentially anywhere and *everywhere*; it can be contested that these kinds of tactics were utilized long before the War on Terror, such as Hitler's construction of the omnipresent 'Jewish threat' in Nazi Germany and similarly, the pervasive 'communist threat' constructed by Western nations in the Cold War era. Mark Neocleous (2003) illustrates the tendency of 'Hitler's Jew' to be "everywhere and nowhere, to be everything and nothing":

> The object of Hitler's fear might be the Jew, then, but it is never *clearly* the Jew, for this object possesses contradictory qualities: a communist intent on overthrowing private property and yet also a capitalist consumed by greed; a figure with too much public influence and yet who retreats into his private sphere; a force behind the institutions of the modern state and yet which also threatens to abolish them once in full control; an avant-garde artist with extravagant and subversive values and yet also a provincial petty-bourgeois white-collar worker; pacifist and yet belligerent imperialist; homosexual ruining strong masculinity and yet seducer of Aryan women. The list of contradictions goes on and on (Neocleous 2005: 73, 74, italics in original).

Thus, while the 'face of terror' trope is useful in illustrating the ongoing intersection of 'race' and security in twenty-first century facial discourse, it is unproductive to dwell on this notion too much in regards to pacification and population management. 'Visualizing the enemy' in this way is a technique of governance that has always - in some way – characterized discourses on war and enemies in the Western modern era. While the theme of terrorism is revisited in chapter 5.1 "'From the Battlespace to the Gene Pool': Facial Recognition for Military, Borders, and Police", it is important to emphasize here that the late-modern relationship between faces and securitization should *not* be reduced to a direct consequence of post-9/11 security measures in relation to the 'dangerization' of members of the Muslim faith through the events of 9/11 and the Global War on Terror. While that is not to discount the racialization of twenty-first century terrorism and subsequently, the many horrific consequences of the War and its effects on that community; or the fact that these events bestowed some new powers to Western law enforcement agencies in policing 'risky' identities (further empowering the hegemony of the database), the contemporary cultural and institutional obsession with such 'risks' - and its relationship to facial discourse - *cannot* be attributed solely to the post-9/11 national security complex (see Neocleous &

Rigakos 2011). As such, it is more effective to situate the contemporary securitization of faciality within the broader context of the unfolding of the *risk society* – a mode of societal governance that preceded the events of 9-11 (almost a decade prior). The following chapter argues that facial discourse in the risk management era has been characterized not through the post-9/11 'face of terror', but rather, through the broader discourse of the unknown and the *unseen* face. While more research needs to be conducted on this topic, the following chapter suggests that security's monopoly over visual representation has lead Westerner's to internalize 'risk' culture and fear those who cannot be subject to identification practices.

4.5 Frightful Facelessness: Facial Obstruction and Individualism in the Risk Society

> Policemen and security guards wear hats with a peak that comes down low over their eyes. Apparently this is for psychological reasons. Eyebrows are very expressive and you appear a lot more authoritative if you keep them covered up (Banksy 2006).

Since the face is bound to narratives of security, the most problematic face is that which cannot be subject to the material gaze and scrutinized. In other words, the *covered face*. In the following passage, Slavoj Žižek (2010) elaborates on the feeling of comfort that comes with seeing human faces – and simultaneously, the uneasiness that radiates from the concealed face:

> [the] face is what makes the Neighbor *le semblable,* a fellow-man [sic] with whom we can identify and empathize…This then, is why a covered face causes such anxiety: because it confronts us directly with the abyss of the Other-Thing, with the Neighbor in its uncanny dimension. The very covering-up of the face obliterates a protective shield, so that the Other-Thing stares at us directly (Žižek 2010: 69).

If we return for a moment to the language and arguments of Deleuze and Guatarri (1987), Zizek (2010) here (without referring to the two scholars directly), is alluding to the 'black hole' of subjectivity that characterizes faciality (as it exists in modern facial discourse). In other words, because the human face as we see it now, *absorbs* (like a black hole) cultural subjectivities such that we invest so much of the individual's humanity into faciality – its obstruction, distortion or absence when visualizing the human body mystifies the identity (and in some cases the humanity) of the individual. If we recall the 'body-head system' characteristic of ancient or 'primitive' societies, as Deleuze and Guatarri theorize, the covered face would signify *only* that there was a head attached to a body; and as this thesis has strived to illustrate, the anxiety generated by the unknown face should be seen as a product of culture, a modern symptom of facial discourse that cannot be divorced from history and politics. While it can be argued that the unknown, unseen or covered face (henceforth facial obstruction) has had a long history in generating fears and anxieties in the Western world, its marriage to images generated by dominant culture and security discourse is a more recent phenomenon (related of course, to the proliferation of optic technologies and media). This chapter argues that the societal preoccupation with risk (which emerged from discourses on dangerousness in the 1970s and 80s) intensified fears of the other such that facial obstruction has become constructed as a problem for security.

A tenet of the risk society is that the risk-conscious population maneuvers themselves through 'safe', 'agreeable' or 'protected' spaces to the best of their ability, adhering to highly policed and surveilled institutionalized settings; this is most often through controlled-for commercial and private spaces through which contexts of action are pre-determined – minimizing the potential chances of victimization (ie: business centres, shopping malls, supermarkets, theme parks, tourist destinations etc.). In these settings the participant becomes "an actor on the security stage" – surveillance renders him or her both *suspect and protected* (Lianos 2012: 32). What must be emphasized here is the policing of visual space in these settings, through which the face becomes subject. The now normative gaze of extensive CCTV networks, pushes the technology of the video camera far beyond its initial role as a security device for identification purposes in 'high-security' settings (such as military areas or bank vaults) (Lianos 2012: 90). As such, video surveillance has become inscribed with certain taken-for-granted cultural implications in the governance of crowds and has consequences on the social conduct of those caught in its gaze. For example, the very presence of a video camera communicates its message: "do nothing suspicious; we know who you are, and we shall have conclusive evidence that you are the one who did it" (Lianos 2012: 106). As a mechanism of discipline which deters certain forms of decision-making, those subject to these institutional modes of governance are aware that they are being watched, and the conforming risk-conscious population takes comfort in this. At the same time, subjects are also conscious that they are suspect to security and may be subject to intervention should they stand out from the homogeneity of the crowd; individuals make an effort blend in, in order to avoid the presumed gaze of the camera (Lianos 2012: 33). This

involves a constant adherence to the institutional habitus, which the following passage illustrates quite nicely:

> Whatever the nature of the establishment, when one is inside, one is presumed to be seeking something that is linked to its function; entering a café automatically creates the supposition of something to do with "a café" and specifically "*this* café" (Lianos 2012: 44, italics in original).

Institutional spaces involve culturally *prescribed* sets of behaviors and norms; when one individual cannot display a precise function or role they become 'de-legitimated' and 'banished' "from the experiential world" (Lianos 2012: 134, 135); loiterers, drunks and the homeless are some common examples of those who become othered through these processes. Those individuals already outside this sphere (those who often constitute the 'likely aggressor'), become the 'absolute other,' as interaction with such an entity "lacks the guarantees of an institutional context which would *structure his* [sic] *relationships in advance*" (Lianos 2012: 132, italics added).

One taken-for-granted aspect of risk management spaces, and one that often escapes discussions of the basic scheme of video surveillance, is the expectation of an exposed face for the disciplinary gaze to 'see' – or in other words, a *material conception of identity* that can be subject to the gaze of security. Across many cultures, the face tends to be one of the least covered surfaces of the body (Negishi 2013: 324), and theoretically, the success of CCTV disciplinary power lies in the belief that should individuals 'stand out', there may be social or legal consequences, as they will be identified through the connection of their visible facial features to the official database (or perhaps the social media database). This recalls again, the idea that "we know who you are, and we shall

have conclusive evidence that you are the one who did it" (Lianos 2012: 106). This ideology is written into the 'common-sense' discourse surrounding CCTV. For example, many of us may be familiar with the popular idiom: 'smile, you're on camera! :)', which is sometimes plastered on wall-mounted posters to emphasize the presence of a CCTV network in a presumed spatial gaze (posters which are becoming less prevalent as video surveillance increasingly becomes a defining feature of social interaction within institutions). Firstly, this phrase assumes that subjects subscribe to the norm of having their face (smile) uncovered. And secondly, that they passively acknowledge the gaze of the camera through which they are both suspect and protected (an idea which is emphasized through other similar phrases such as 'you are being monitored for your own security'). As such, it can be argued that facial exposure is a social expectation of the late-modern institutional habitus. To conceal the face in these settings - unless there is an immediately obvious reason *not* to do so (such as concealment under a scarf in cold weather) – is to contest the visual authority of the camera and thus immediately draw attention to oneself – to become a risky individual. As Lianos (2012) puts it, in such an atmosphere even the slightest deviations become scrutinized: "the inevitable result is a very broad definition and an increased fear of anything that does not fit into this well-managed homogeneity" (33).

It is perhaps no coincidence that throughout the emergence of CCTV networks and the risk society – with the latter starting in the mid-1970s through the emphasis on 'dangerousness' – that popular Western horror films began to associate facial obstruction with violent and murderous individuals, emphasizing terror in the *unknown*. While earlier films such as Alfred Hitchcock's *Psycho* (1960) certainly invoked horror through the

unidentifiable murderous character-type, 1970's horror film began to emphasize the spectacle of the covered face in conjuring these fears. In such pieces, the purveyor of violence is clearly visualized on the screen, but their face is hidden from the audience and the onscreen characters, often through a mask (in many cases, the mask *becomes* the identity of the individual). One might argue that the 1925 film *Phantom of the Opera* plays off of the spectacle of the masked individual, however, the concealing of the 'phantom' character's face (Erik) is not necessarily a tool to evoke fear in and of itself, but rather, the primal fear is arguably evoked when Erik's face is revealed to resemble a corpse (which fits with the monster movie trend of its time). On the other hand, films such as *The Wicker Man* (1973), *The Texas Chainsaw Massacre* (1974), *Alice, Sweet Alice* (1976), *Halloween* (1978), *Friday the 13th* (1980), *Curtains* (1983), *Stage Fright* (1987), *Silence of the Lambs* (1991) and *Scream* (1996), are only a few examples in Western cinema, through which the obstructed or concealed face becomes a spectacle of terror in and of itself. In many of these movies, the 'facelessness' of these characters performs as an extension of their violence and deceit. For the violent individual to conceal their facial traits from both the onscreen characters and often the audience, means that 'the killer' can simultaneously be everyone and no one – arguably reinforcing individualist cultural values whose motto is "trust nobody". The insecurities generated by the risk society have fostered a stark individualization where 'trust is eroded at every turn'; as Bauman explains (invoking the language of Ulrich Beck):

> Individualization amounts to 'the experts dumping their contradictions and conflicts at the feet of the individual and leaving him or her with the well-intentioned invitation to judge all of this critically on the basis of his or her own notions' (see Beck 1992, cited in Bauman 2001: 105, 106).

In a society where media and politicians "insist on the advent of a newly dangerous, uncertain world" (Lianos and Douglas 2000: 261), and through which the citizen-subject is repeatedly told that he or she is the master of his or her own fate and is accordingly made responsible for his or her own safety and security (Bauman 2001: 107); distrust of the other becomes a rational calculation for the conforming risk-conscious individual. And while crime and violence make up only a small component of the risk management process and the insecurities faced by late-modern subjects, they are useful analytical tools for illustrating the influence of media, experts, and dominant interpretations of otherness more generally. For the media, "crime consists almost entirely of violent acts between people who do not know one another" (Lianos 2012: 128); and as a 1988 study has shown, films or TV series contain on average "one act of violence every ten minutes", through which a young person of 'average sociodemographic profile' may have seen an estimated 26, 000 murders by the age of 18 (Cumberatch 1988: 12). Considering this data, it is not difficult to see why it is the least victimized groups that are often the most afraid (Clemente and Kleiman 1976; Garofolo 1981) (groups which of course, have the privilege of both accessing and spending time with this form of entertainment). Thus, for the conforming majority (the 'privileged core' of society as Lianos puts it (85)), the fear of being a victim of crime must be understood in connection with the person's *private life*, "since it is, firstly, the body and the spaces that are exclusively intended for it that are the target of the projected threat" (Lianos 2012: 125, 126).

The post-war preoccupation with violent crime – stemming in many ways from the proliferation of televisual culture – is arguably why spectacular displays of violence

in the horror genre continue to be pertinent. It is worthwhile to consider some of the cultural implications of this film genre and its relationship to faciality and violence in dominant culture, as the medium has been analyzed in the past to expose certain political and cultural trends, or as Newman (1988) puts it: "the horrors and neuroses of the age" (211). For example, Neocleous (2005) explores the classic German horror film *Nosferatu* (1922) (an unauthorized adaptation of the novel *Dracula*) and its relationship to the political climate of National Socialism in Germany. In the film's depiction of a traditional German town under threat from a foreign creature, Neocleous (2008) argues that there are deep anti-Semitic undertones consistent with the 'fascist imagination' (88), particularly when the film emphasizes the *foreignness* of the creature. In conjunction with the very *appearance* of Nosferatu (or 'Count Orlok'), the character is constructed as "a pestilence which comes in the form of a sexually predatory blood-sucking and property-developing tyrant looming at the borders of the nation" (87). As he elaborates:

> [*Nosferatu*] remains a fundamental expression of the kinds of fears which preoccupied nationalist, racist and anti-Semitic tendencies during the period… Films like *Nosferatu*… helped establish the cultural, ideological and visual context - a Gothic context - for the racial melodrama that the Nazis were about to unleash on Europe (Neocleous 2005: 87).

As such, it is important to consider the expressionism and symbolism in such 'cultural productions' as they potentially both construct *and* reflect a certain political atmosphere.

The horror film genre relies on eliciting a negative emotional response from viewers by exploiting the audience's fears; Pinedo, a scholar of film and media posits that:

> Horror is produced by the violation of what are tellingly called natural laws, by the disruption of our presuppositions about the integrity and predictable character of objects, places, animals, and people (Pinedo 1996: 20).

The fears exploited in these films are historically and culturally contingent as they involve portrayals of violence that disrupt the world of everyday life and 'explode our assumptions about normality'. Pinedo (1996) uses the simple example of *Dracula* and *Night of the Living Dead* in which the "impermeability of death is violated when corpses come back to life" (20). Studies on the horror genre tend to focus on the psychological aspects of provoking fear and discomfort, but it is sometimes taken-for-granted that the medium of film relies on *visual* storytelling – this is especially true for horror films as they often rely heavily on imagery itself to provoke an emotional response (see Powell 2006). Taking the face as the object of study, this section is interested in the implications of the *aesthetics* of the horror genre and portrayals of the monstrous. In a nutshell, horror films involve violence perpetrated by a monstrous entity:

> Horror violates the taken-for-granted "natural" order. The anomaly manifests itself as the monster: an unnatural, deviant force. The monster violates the boundaries of the body through the use of violence against other bodies and through the disruptive qualities of its own body. The monster's body dissolves binary differences. It disrupts the social order by dis solving the basis of its signifying system, its network of differences: me/not me, human/nonhuman, life/death (Pinedo 1996: 21).

'Classical' horror films traditionally provoked the viewer's fright through the visual portrayal of literal monsters such as those figures seen in *Dracula* (1931)*, Frankenstein* (1931)*, Dr. Jekyll and Mr. Hyde* (1931); this trend later became known as the 'creature feature', which continued well into the 1950's with films such as *The Thing* (1951),

Invasion of the Body Snatchers (1956), and *The Blob* (1958) (see Pinedo 1996: 19). While movies involving nonhuman creatures is less a commonplace following the 1960s and 1970s, the movie monster trend has not come to a halt, instead, it can be argued that much of the 'monstrous violence' of the horror genre has shifted from the inhuman to the human – through the portrayal of monstrous people and identities. As Pinedo (1996) points out, film-makers recognized they could evoke fear by drawing the danger closer to home (19); as such, the monstrous violence in popular features of the late 1960s, 1970s and onward became perpetrated by less exotic entities: "the psychotic killer's inexplicable violent rampage. . .supplanted the traditional monster of castles and closed endings" (20). The monstrous figures of late-modern horror began to infiltrate some of the most (perceived) secure spaces and settings of the private sphere, such as in the home in *Halloween* (1976), a high school in *Scream* (1996), and of course in the broader sense, such monsters ruptured the comfort that we take in the local (neighbourhood and community). It was at this time – in the mid- 1970s - that the horror mask became a central facet of this genre, with many of the aforementioned pictures such as *The Texas Chainsaw Massacre* (1974), *Halloween* (1978), *Friday the 13th* (1980) and *Scream* (1996) arguably becoming some of the most influential horror films of their time. And while the horror-mask can be seen as a tool/plot device for the filmmakers to generate mystery and suspense for the viewers, or as a gimmicky visual marketing tool, it is not unreasonable to argue that the sudden advent of the horror mask reflected dominant ideas surrounding faciality and its relationship to an increasingly securitized identity. By dawning masks and (in often cases) infiltrating 'secure' spaces, these new monstrous figures contested the hegemony of facial identification and the taken for granted security of the disciplinary

gaze. In other words, with the intensifying marriage of faces to security (reinforced through state documents, institutions and social transactions monitored by CCTV), the concealing of one's face became a horror in itself. To hide the face was to reject the central corporeal component of liberal identity (ie: the dominant culture's construction of faciality, which is derived from the state); or as Delueze and Guatarri (1987) would put it, covering the face erases the historical legacy of "significance and subjectification" which dominant culture has transcribed upon it (188) – "the mask erases the old subject and represents the new subject" (Avery-Natale 2010: 102).

Interestingly, what also distinguishes the late-modern era of horror film from the classics is the refusal of narrative closure (Pinedo 1996). Unlike classical films where "male military or scientific experts successfully employ violence and/or knowledge to defeat the monster and restore the normative order" (Tudor 1999: 81-105), in late-modern features the monster triumphs, and the result is an "unstable, paranoid universe in which familiar categories collapse" (Pinedo 1996: 19). Additionally, the iconography of the human body figures as the site of this collapse (Pinedo 1996: 17).

While more research needs be conducted on the relationship between the horror medium and its socio-cultural implications, it can be argued that these types of films, by associating facial obstruction with the threatening, the disturbing, the unknowable, the unpredictable, and sometimes the inhuman, reinforce the 'black hole' epistemology of faciality, such that to conceal one's face is to literally conceal your identity – or perhaps more accurately, to replace your identity with a 'risky identity', to become the 'other-thing' that must be avoided at all costs. Additionally, to construct the concealed face as something which is inherently risky or 'monstrous', is to award authority to video-

surveillance culture and state narratives of identity and faciality, both of which emphasize exposed faces as the optic centerpiece of those discourses. Anything else becomes a security issue.

While it might be a stretch to argue that the horror-mask film style has had a significant cultural impact on late-modern individualism and interpretations of facial obstruction and its relationship to 'stranger danger', it can at least be stated that the fears exploited in these popular films must in some way *reflect* certain dominant ideas about faciality, identity, crime, violence, victimization and risk; ideas which persist well into the present. And if the enduring popularity of the horror-mask genre is demonstrative of anything, it follows the ongoing argument of this project, that Westerners *depend on discourse and culture* in both *seeing* the face and *knowing* identity; and subsequently, this illustrates that both our faces and our identities are subject to historically contingent modes of thought, implicating that in the late-modern era we have little control over how our faces are seen and how our identities are projected.

Chapter 5: Facial Recognition as Pacification

5.0 Facial Recognition as a Biometric Technology

Introduction

In theory, facial recognition software has the potential to be the technological apex of liberal governance as it augments the very infrastructure of Western surveillance regimes

through its direct appeal to the bedrock *logic* of liberal identitification practices and their relationship to security and the spatial gaze. Definitively, it 'governs at a distance' while simultaneously maximizing discrimination in the name of order. In other words, without reinventing the system, FR software exploits the exterior and interior transparency of those individuals subject to a spatial gaze, through which a security mechanism can then be exercised in a controlled atmosphere (such as systems of access or exclusion - as in an airport), or through which target marketing can be deployed or metadata be created (such as through the tracking of movement or in 'seeing' gender or age). In a culture where information *about* the body is being treated as if it were conclusive in determining the *identity* of the person (Lyon 2013: 134), FR appears to be the next logical step in facial identification practices - in the historical project of identification as pacification. The potential streamlining capabilities of FR (particularly in regards to automated identification) make it desirable as something which can increase proficiency by reducing or replacing human labour in a number of different ways (such as replacing door security or combatting labour by automatically sorting through video footage). While the technology is still fairly new and its capabilities remain largely inadequate outside of controlled settings, the demand for FR is growing substantially among both state institutions and the corporate sector (see Jones 2014). This chapter explores all of these themes in much more detail. The following section looks at the history of facial biometrics and its relationship to other forms of biometric surveillance technology.

Defining 'Biometrics'

Facial recognition technology is a form of *biometrics*, a term which Denham (2012) defines as follows:

> [biometrics is] literally, the measurement of life. It refers to the technology of measuring, and processing the digital representations of unique biological data and behavioral traits such as fingerprints, eye retinas, irises, voice and facial patterns, gaits, body odours and hand geometry (Denham 2012: 7).

Denham's (2012) definition, while useful in illustrating biometrics' comprehensive forms, does not do enough to emphasize its marriage to mechanisms of surveillance and identification. As such, in addition to digital measurement, it is necessary to incorporate into this definition: the recording and monitoring of parts of the body (Tudge 2011: 91, Lyon 2001: 72 cited in Aas 2006: 145) through which a person's unique 'physiological characteristics are used to verify or establish their identity' (Aas 2006: 145). By programming machines to literally 'see' identity by observing parts of the body, biometric technologies reproduce dominant relationships of power by bestowing authority to the logic of liberal identity politics (which rely on a materialist conception of identity). As such, state-security narratives are written into the very fabric of biometric technologies, which anchors them as a dynamic, yet inconspicuous political force.

In their inception, biometric technologies promised to "stabilize the messy ambiguity of identity, to automatically read a stable, individual identity directly off the body" (Gates 2011: 14); and in the liberal fashion, such mechanisms were initially applied to populations with 'suspicious or disreputable social status' (Aas 2006: 146).

Early stages of digital fingerprint identification and DNA testing for example, were largely exclusive to criminal populations. Some attribute the emergence of biometric technology in the public sector to the intensified risk-security atmosphere which followed the attacks of September 11 and the subsequent attacks in Europe. Lyon (2003) argues that these events brought to the surface a 'number of surveillance trends that had been developing quietly and largely unnoticed for a decade earlier'. Biometrics appealed to both state and commercial institutions as the technology promised to enable the intensification of identification practices at a proliferation of sites – a priority which had gone hand-in-hand with the political-economic and governmental atmosphere of neoliberalization (Gates 2011: 27). As Aas (2006) delineates, touching on a number of themes discussed previously:

> . . .the growth in biometrics should be understood as part of a general trend towards identity management and the 'securitization of identity', exemplified by rising concerns about terrorism, asylum and migration, identity theft and identity fraud (Aas 2006: 146).

While this essay does not share the same interpretation of the 'securitization of identity' outlined by scholars such as Aas (2006) and Gates (2011) – and coined by Nikolas Rose (it would be more accurate to term such a process as the 'securitization of identity *documents*'), Aas' is correct to locate the growing appeal of public-sphere biometrics as the inevitable outcome of risk management culture and its relationship to the insecurities generated by identifying and governing risky individuals. Following the history outlined in this essay, biometric technology should be seen as the next logical step culminating from the liberal identification process, *not only* as a product of the 21st century national-

security environment. However, while we must be careful to avoid placing too much emphasis on the post-9/11 security climate in discussing the proliferation of biometric technologies, it is not unreasonable to suggest that the political ramifications of the 9/11 attacks and the Global War on Terror accelerated this process through 1) budgetary increases in national security initiatives, 2) furthering the merger of private security and the state, and 3) by fostering a political environment through which these technologies could flourish.

Facial Recognition: How it Works

In industry language, facial recognition software is a form of *video analytics* (VA), which simply refers to automated or semi-automated technology that analyzes live or recorded video footage (this term was used frequently at the "Biometrics for Government and National Security" summit). As such, when facial biometric algorithms are implemented into video surveillance networks, it is often referred to as "smart CCTV". Firstly, facial recognition technology involves applying computer algorithms to digital photographs or video stills to measure the distance between the eyes, nose, mouth and cheekbones (although different programs have slightly different techniques) (Tudge 2011: 97). Newer programs also involve the measuring and shape of the ear(s), especially when analyzing side-profiles (see Bourlai 2014). The second part of facial recognition technology involves comparing these measurements to images captured in a digital database; these are images which are most often formatted to accept the software. A match is made through likening the initial images' translated code to the code of a facial image within

the database. Bruegge (2010), one of the leading forensic examiners in the FBI's 'Biometric Centre of Excellence', breaks down FR technology into these two parts; between FR, referred to as automated searching and evaluating of facial images within a computer database, and 'facial identification' – FI, referred to as "*manual* examination of the differences between two facial images for the purpose of determining if they represent different persons or the same person" (Bruegge 2010: 3). Bruegge (2010) argues that the future of 'identity intelligence' lies in making this connection more seamless.

History of Facial Recognition and its Relationship to Other Biometric Forms

> Indeed in the security world the perfect unobtrusive biometric is considered the 'holy grail' (Introna & Wood 2004: 178).

From an analytical standpoint, the early history of facial recognition technology is rather unremarkable and has little to offer beyond its political roots in the themes discussed in the previous chapters. The technology emerged in the late-1960s following the public and private sectors' recognition of an intensified need to deal with the problem of 'a proliferation of disembodied identities' residing in databases and circulating over networks (Gates 2011: 26). As part of the concerted effort to make identity orderly, a number of research labs emerged around this time in the United States, funded by the Department of Defence and various intelligence institutions. In these laboratories computer scientists began working to 'train' cameras to see human faces. This was happening in other parts of the world as well, particularly in Japan, where one of the first

displays of FR software was exhibited at the 1970s World Fair in Osaka; participants were asked to have their picture taken, through which the program would compare their image to a database of celebrities, displaying which famous individual they looked most alike (Gates 2011: 25). These early programs were largely unreliable; as Gates (2011) notes, understanding the 'physics of vision' was more difficult than anyone had initially realized. Locating a face in an image was a significant obstacle to overcome as this involved translating a 'flat' 2D visual into a 3D plain inscribed with cultural significations (Gates 2011: 25, 31). Subsequently, it was not enough for this software to simply measure facial features and process information – FR technology had to incorporate a degree of artificial intelligence through which cameras could not only problem-solve, but also *perceive* the world as a human does (Gates 2011: 31, 32). Even after returning to the basics and reinventing the foundation of facial biometric algorithms, the technology was still 'ahead of its time': "in the sense that the technologies it harnessed, computers and video cameras, weren't advanced enough to make it work, especially when it came to replicating in the field what was done in the lab" (Mockenstrum 2002: 110). And as it stands now, most of the algorithms in facial recognition are based on "very sophisticated statistical methods that only *a handful of experts can interpret and understand*" (Introna & Wood 2004: 183, italics added). This ongoing struggle to 'see' – or rather *construct* - the face is further demonstrative of Deleuze and Guatarri's (1987) assertion that 'the face is a politics'.

For the above reasons, the progression of FR technology was a slow process and these research programs did not gain much momentum until the commercialization of the software in the 1990s. While FR technology continued to be mired with seemingly

endless logistical and technical challenges, its capabilities were certainly improving, and what it *promised* to deliver became increasingly relevant to the socio-political atmosphere (outlined throughout the preceding historical analysis). As Tudge (2011) points out, progress in biometrics – especially for facial recognition - had not been defined by proficiency, but by profit (Tudge 2011: 97). Gates (2011) encapsulates this quite well in the following passage:

> Facial recognition systems promised to build on existing identification infrastructures to refashion face-to-face forms of trust and recognition for official identification in mediated contexts. The primary aim of these systems would be to deliver concrete, practical benefits in the form of more accurate, effective, ubiquitous systems of facial identification that operated automatically, in real time, and at a distance (Gates 2011: 28).

These 'practical benefits' unique to the visual aspect of facial biometrics are what made the technology stand out from the 'tried and true' methods of other biometric forms – most notably digital fingerprinting and DNA sampling. Even in controlled atmospheres, FR software was not nearly as accurate or reliable as these technologies, which continues to be the case (Tudge, 2011: 98; Gates 2011: 17). However, the desirability of FR software lied precisely in its inconspicuous and cost-efficient implementation in the CCTV-saturated public sphere. Despite the fact that we all became suspect in the world of risk management, many individuals took offense to being fingerprinted 'like criminals' (Tudge 2011: 93); and although DNA biometrics were the most potent and trusted of all biometric identifiers, their usage was also the most intrusive, personal and violating (Tudge 2011: 98). As a more complex and specialized method of identification – lacking any sort of immediacy between identification and the presence of the subject, DNA

samples were also vulnerable to being "planted at crime scenes…mislabeled, badly filed, [and] inadvertently mixed or contaminated with DNA from elsewhere" (Tudge 2011: 99). Perhaps most significantly, application of these surveillance mechanisms required direct contact and cooperation by their subjects – in short, conspicuous touching of the body.

However, this is not to discount the escalating user acceptance of some of these biometric technologies over the last decade, particularly digital fingerprinting. In addition to fingerprint biometrics seeing growing popularity as a security measure for phones and other consumer devices; digital fingerprinting units have been installed in a number of areas across the West, particularly in airports and tourist attractions such as at the gates of Disney's Universal Studies Orlando and at the Statue of Liberty in New York City (Crompton 2014; Cosgrove-Mather 2004). Six Flags theme parks in the United States and Canada even offer a 'Biometric Season Pass' through which customers can provide their biometric fingerprint information, replacing the traditional physical season pass card (SixFlags.com 2014). The benefits of this lie in making the identification process more efficient and orderly by solving the problem of lost or stolen cards. Another benefit lies in reducing human labor through the replacement of gate security personnel with stationary fingerprint-reader units (although these stations often require human supervision to account for technologically-inept individuals and biometric-reading errors). In another example, 'Smart Carte Inc.' has developed 'fingerprint lockers', a system which has replaced traditional key-locker units at many of these locations - in addition to a number of airports and railway buildings in the US. Similarly, these systems have been implemented to address the issue of lost keys, a previously common problem which

hindered parts of the security apparatuses in these institutions (see Cosgrove-Mather 2004).

While fingerprint recognition has been described as the 'backbone' of the biometrics industry (Vemury 2014) due to its history (as one of the first biometric identifiers), accuracy and availability, other technologies have been on the rise as well. Palm recognition for example – the 'Handpunch' system - has been installed at a number of McDonald's restaurants in the US, Canada and Venezuela in an effort to thwart 'buddy punching' – which refers to when one employee punches into an attendance system on the behalf of a tardy or absent employee (Journalistic Inc. 2014; Ingersoll Rand 2009). Additionally, iris recognition (IR) has been growing in popularity as well, and the technology is far more accurate than facial biometrics (and also more accurate than 1-print fingerprinting). However, because IR requires the installation of a unit (more expensive than fingerprinting), and active participation by the subject, its presence in the commercial realm is rather underwhelming and buyers of IR technology have been limited largely to state institutions, airports, and the prison system. The District of Columbia Department of Corrections for example, has been interested in installing IR technology as a supplementary security measure, in order to prevent the release of the wrong inmate (a surprisingly common problem) (Bohmer 2014; Vemury 2014). Lastly, DNA sampling remains the most accurate and reliable biometric identifier and has improved dramatically since its inception in 1984. At that time it took seven weeks to process a 'six loci result' (a locus - loci plural - refers to an isolated chromosome), in 1998 it took three days to process a thirteen loci result, and in 2012 only ninety minutes to process a thirteen loci result (Loudermilk 2014). As James Loudermilk (2014) of the

FBI notes, the current focus of this technology is to enhance its reliability and cost efficiency, as opposed to improving its speed.

In addition to facial recognition, the preceding technologies are the most popular biometric processes of the present. Other biometrics that are lesser used or are currently in the works are handwriting, gait (body motion), tattoo, vein, voice, ultrasound and scar/skin-mark recognition (Loudermilk 2014). Scent recognition is perhaps the most unusual, a technology program which materialized as an effort to replace police canine units. As Loudermilk (2014) explains, the incorporation of 'drug dogs' into law enforcement has been met with a number of issues. The dogs must be cared for and fed; and because the dogs are paired with a single trainer, should the trainer or the dog die, or should the officer leave the force, a new dog must be trained (and the previous one must be put down). Scent recognition technology has been seen as a potential answer to these budgetary and efficiency issues.

In order to illustrate the varying capabilities and efficiency of the numerous and diverse biometric forms, Loudermilk (2014) provides a very useful chart (***Figure 1***) which locates each biometric technology according to 1) its accuracy/reliability and 2) distance/range – in other words, the amount of contact and participation that the subject must provide. Tellingly, the chart locates just about all of the aforementioned technologies as requiring a substantial degree of cooperation on part of the subject, with the exception of FR software and gait recognition. Gait recognition technology, however, is still in its infancy as no model has, as of yet, been developed that is sufficiently accurate and marketable as a security mechanism; it is predicted that in the future (an estimated five years), gait recognition will likely be applied in conjunction with other

biometric forms to identify individuals (Global Security Intelligence 2014). FR on the other hand, has seen dramatic improvement in accuracy and reliability over the last two decades. From 1995 to 2002, the technology has become one-hundred times more efficient; from 2002 to 2007 it has improved tenfold (Williams 2007) and from 2007 to the present, FR accuracy has improved threefold (Bourlai 2014). In addition to this, the 'notional range' of FR technology, as previously outlined, is what has made it stand out as a 'prime focus' for the security establishment (Introna & Wood 2004: 178). FR is potentially the 'holy grail' of biometrics because of its characteristic as a 'silent technology', which is what distinguishes FR from most other biometric forms - which Introna and Wood (2004) describe as 'salient technologies' (for example, software versus hardware, hidden versus conspicuous, passive versus active operation, etcetera) (183). The application of FR is flexible and entirely passive in its operation: "It requires no participation or consent from its targets – it is [a] 'non-intrusive, [and] contact-free process'" (Introna & Wood 2004: 183). What is not emphasized by Introna and Wood in this discussion, and must not be overlooked, is that FR *does* require a behavioral component (as indicated in Loudermilk's chart) – namely, the acquirement and storing of the subject's photograph from which to compare the captured video footage. However, this behavioral component is not necessarily a hindrance for FR implementation and arguably makes up a central part of its allure, as the following will explain.

The face is the "most common biometric in use by humans to identify other humans" (Introna & Wood 2004: 178); as such, even beyond the photo identification of official databases, FR has the potential to exploit the tremendous digital expanse of photo-saturated Internet culture. As Haggerty and Ericson (2006) posit, Western nations

can be described as 'viewer societies', emphasizing the culturally powerful practice of *watching* (28). Lyon (2006) expands on this notion using the term 'scopophilia' (the love of looking) through which he argues that the current appeal of surveillance technologies is related to 'the scopophiliac viewer gaze' where: "Viewing is now positioned as an intrinsically pleasant act, and the love of watching has ushered in yet more surveillance and monitoring" (Lyon cited in Haggerty & Ericson 2006: 28). Bauman makes a similar observation where he asserts that "everything private is now done, potentially, in public – and is potentially available for public consumption" (Bauman 2013: 22). Bauman encapsulates this cultural shift quite well by pointing out that the 'panoptical nightmare': 'I am never on my own' and 'I am always being watched', is being overrun by the 'joy of being noticed' (Bauman 2013: 3). While chapter 5.2, "Consumer Transparency and Commercial Facial Recognition Technology" explores the viewer society and subject visibility in more detail, this section has attempted to position FR software as the centerpiece of contemporary biometrics through its unprecedented capability as a 'silent technology' that complements the surveillance demands of the present, in addition to its potential to exploit the firmly-anchored facial discourse which permeates institutional apparatuses and digital culture. The following section explores its current implementation within controlled an uncontrolled atmospheres by law enforcement and institutions.

5.1 "From the Battlespace to the Gene Pool": Facial Recognition for Military, Borders, and Police

> We are using biometrics to *fix* identity (Boyd 2014, italics added).

> With cameras everywhere, we must exploit that information in order to help with investigations (Bourlai 2014).

At the "Biometrics for Government and National Security" summit in Washington DC in February (2014), John Boyd, director of Defence Biometrics and Forensics at the Institute for Defence and Government Advancement (IDGA), stated that since the attacks on 9/11, the military has been involved in what he describes as 'irregular warfare'. As he explains, the days of 'the cold warrior' are over, enemies can no longer be identified through their uniform or physical placement on a concrete battlefield. Stripped of that identity, the enemy is capable of blending in; and from an 'access control standpoint' (referring to access to security-sensitive areas), this development requires a paradigm shift from the "battlespace to the gene pool" (Boyd 2014). Subsequently, the Department of Defence (DoD) is interested in utilizing biometrics to 'create a unified definition and scope for identity'. The central priority of DoD biometrics, as he continues, is to build a 'sustainable enterprise' through which a more 'holistic identity' concept can be maintained and applied, as identity is "critical to both national security and routine business functions within the department" (Boyd 2014).

For Western governments, biometrics have become the definitive technology for identity security in the 21st century. Mark Greene (2014) - a program manager of biometrics at the National Institute of Justice – argues that biometrics are the driving

force behind "the development of highly discriminating, accurate, reliable, cost-effective and rapid methods for identification". According to Shonnie Lyon (2014) of the Department of Homeland Security, and John Mears (2014) of Lockheed Martin, the overarching objective of such identification systems is to "enable risk-based security"; to "identify risk, reduce risk, and mitigate risk". In addition to this, biometric industry revenue, according to Dalton Jones (2014) of the Defence Intelligence Agency (DIA), is expected to grow from $8.1 billion (USD) as of 2014 to $16.7 billion as of 2017. Interestingly, Jones (2014) locates biometrics as a central new feature in the identification process, dividing human identity into three key elements: 1) *biographical* (passports, travel records, driver's license, finances, property records), 2) *behavioral* (social media, online profile, affiliations, interpersonal networks) and 3) *biological* (fingerprint, voice, DNA, face, iris) (see ***figure 2*** for a more detailed outline).

While state departments such as the DoD are interested in utilizing every biometric technology at their disposal, Western governments – specifically military, immigration/border and intelligence agencies - remain the largest buyers of FR software. It is important to reiterate here that the development of FR technology is carried out largely through private institutions since its commercialisation in the 1990s. As Loudermilk (2014) explains, like the technology of the cellphone before it, biometric technology develops through a "looping feedback" between the commercial sector and government. In the US for example, private institutions work very closely with state departments. Iana Bohmer, the senior specialist leader of 'Enterprise Risk Services' at Deloitte - a massive professional services network that operates internationally - claims that the Obama administration "wants identity security to be led by the private sector"

(Bohmer 2014). Also worth noting, is that because biometric technology is still undergoing constant development (especially for FR, in developing algorithms for uncontrolled conditions), universities – particularly in the US - have been actively involved in this process as well. It is of course, no secret that a number of American university programs have become think tanks for the private security sector and the military industrial complex. For example, the Center for Identity Technology Research (CITeR) is a biometric research program made up of five universities and describes itself as an "Industry/University Cooperative Research Centre". The research of CITeR is funded and *decided by* government institutions not limited to the DoD, FBI, NSA and the US Army, as well as 'industry affiliates', such as Microsoft, Aware, Lockheed Martin, Borders, and Booze Allen (Rissacher 2014); Booze Allen if we remember, is the private security firm that hired Edward Snowden, the individual responsible for the ongoing NSA leaks since June 2013. CITeR is currently involved in approximately 200 projects, from tattoo and iris recognition to infrared facial recognition and 'deception detection' (lie detectors that read body movement) (Rissacher 2014).

Facial Recognition for (US) Military & Borders

> If we don't figure out how to incorporate biometrics into everything we do to include cross leveling and sharing our information between law enforcement, military, and at least our closest allies, we will miss critical information that could save lives (Major General M.T. Flynn 2011, director of the DIA, cited in Jones 2014).

For defence institutions, border and intelligence agencies, facial recognition is most commonly used *in conjunction* with other biometric forms – particularly iris scans and/or

fingerprints. This is because biometrics are often utilized by these agencies as a *supplementary* security technology. For example, they may function as an additional layer of security for highly-sensitive access control points, or as a supplementary identification mechanism for individuals on a watchlist (which follows the logic of Jones' (2014) diagram - figure 2). For instance, the DoD is currently developing a 'mobile identification program' which involves an iPhone sled for military field use. This device integrates fingerprint, iris, face, and voice data for "tactical collection, matching, storage, and sharing" (Boyd 2014). On a side note, when asked who was producing the technology, Boyd maintained that such information was classified; however, it would be unsurprising if the Apple Corporation itself was involved in developing the sled, as NSA documents leaked by Edward Snowden regarding the PRISM program, revealed Apple Inc.'s enthusiastic cooperation with the US government in data sharing and collection (see Ackerman 2014). Another program that utilizes multiple biometrics, also based in the USA, is the Automated Biometric Identification System (IDENT for short), which seeks to improve the US government's ability to track and identify national security threats; the system currently holds biometric information for more than 165 million individuals, in addition to a watch list of 7.5 million people (S. Lyon 2014). While IDENT is primarily a fingerprint system (tracing back to 1994), the demand for biometrics is increasing rapidly and the database is beginning to incorporate new modes of identification, particularly facial and iris recognition technology (S. Lyon 2014). There are numerous other programs similar to the IDENT that stretch across US state departments, such as the DoD's Automated Biometric Identification System (ABIS) and the Biometric Enabled Watchlist (BEWL), a database which currently holds biometric

data of over 48 million individuals (Ratha 2014). Additionally, the FBI's biometric database carries information on over 106 million individuals (Loudermilk 2014). As Jones (2014) posits, biometric information is being collected every day, and there must be a 'constant communication' across these departments to manage and apply this data efficiently.

In addition to general identification and watchlist programs, facial recognition technology is being applied by these departments at gate access points and borders. One project for example, titled rather uncreatively as 'Rapid Biometric System for Physical Access', involves an automated system for "rapid verification of individuals in a vehicle" for DoD access points. As Boyd (2014) outlines, this research effort seeks to deliver "several high-speed cameras that provide a continuous stream of high resolution facial images for matching". The DoD spends more than 100 million/year on gate guards; and subsequently, the purpose of this project is to 'increase performance and decrease cost' (Boyd 2014). The DoD is currently working on 'robust FR software' that seeks to overcome occlusion, pose angle, lighting variation and motion blur for this purpose.

The most common application of FR - across the board - is through the implementation of 'e-gates' at borders throughout the West. As Mears (2014) of Lockheed Martin outlines, these gates are also known as 'Automated Border Control' (ABC), which utilize both facial recognition and/or fingerprint scanners to identify passengers. To a lesser extent, other e-gate types use facial recognition in conjunction with iris recognition. As the title implies, these gates are automated and therefore require no attendant, however, a PSA agent may be deployed for support and technical issues. According to Mears (2014), ABC gates were originally implemented in 1998 in Hong

Kong, and there are now thousands of units installed across Southern China. A number of e-gates have recently been implemented at the Canadian-American borders as of February 2014, and there are multiple airports in Europe that utilize this technology as well. This program is arguably one of the reasons why photos for Canadian and American passports have been formatted to accept FR technology; and similarly, numerous Canadian cities and various US states have begun restricting smiling for driver license photos in order to comply with this process (and future FR projects of law enforcement) (Mears 2014).

The demand for e-gates lies broadly in 'facilitating commerce' (Vemury 2014) by decreasing congestion through reducing waiting times at control points; and by 'increasing revenues by getting travellers quicker to the retail area' (Vision-Box 2014). As Arun Vemury (2014) of the Department of Homeland Security notes, the implementation of ABCs in the US/Canada has been particularly slow due to processing issues and infrastructure; "technology is not really the problem". The problem lies in implementing ABCs without impeding airport operations or interrupting business models (nearly all airports in the US and Canada are privately owned). As Vemury (2014) notes, the implementation of this technology must be seamless, as "we don't want to put anyone out of business" (although they do not appear to have a problem with cutting labour or the potential layoffs of gate-security personnel). In addition to widespread implementation, the future priorities of ABC units, as Mears (2014) concludes, is the incorporation of additional biometrics – particularly iris scanning – as well as enhancing facial recognition to operate at a greater distance and on the move (Mears 2014).

Local Law Enforcement and Other Applications: The Limitations of Uncontrolled Facial Recognition Software

We must be careful not to draw too much of a distinction between 'controlled' and 'uncontrolled' FR systems as the line is never that clear due to the myriad of variables that affect facial algorithms (the DoD's 'Rapid Biometric System for Physical Access' is an example that blurs such a distinction). However, we can safely say that the preceding examples of applied FR technology are largely conducted in 'total institution' environments, encompassing knowing and/or consenting subjects. Subsequently, because the individuals being identified are largely cooperative in providing their biometric information, while also subject to largely controlled and supervised conditions – ie: governed by signs/directions, personnel, appropriate atmosphere/lighting, clean indoor cameras, high-definition video recording, etcetera - many or most of FR's limitations can be overcome. The accuracy of FR technology in such an atmosphere is in the lower 90% (Loudermilk 2014). In less controlled or 'uncontrolled' conditions however, the accuracy of the software often plummets – although this is highly dependent on a number of variables.

We can define an 'uncontrolled' setting - broadly - as any spatial gaze subject to video recording technology that that does not explicitly involve interaction on part of the subject and/or explicit consent. A ('smart') CCTV network is perhaps the most obvious example of this. Under *un*controlled circumstances, facial algorithms become complicated by a number of potential factors, making it much harder to match the live imagery or recorded video still to a 'controlled for' image in a database (most often a

mug shot). The most common problems, as outlined by Thirimachos Bourlai (2014), a leading expert on facial algorithms (and researcher for CITeR), are illumination, pose variations (angle), age, exaggerated facial expressions (smiling, frowning, open mouth, face scrunching), noise (image quality), facial obstructions, as well as the location of cameras. It is important to outline these limitations in more detail. For many CCTV networks for example (particularly older systems), camera placement is often *above* individuals and FR software works best when the subject is facing the camera directly (Bourlai 2014). Similarly, pose variations are a common problem, as side profiles for instance, do not provide all the biometric information necessary to make a match (3D facial imaging and ear recognition are being developed as part of the solution to this). Also, age is a variable that is particularly problematic as of course, faces change with time, some more drastically than others – the development of wrinkles may affect the algorithm and subsequently, the matching process. Another central problem is the amount of 'noise' in a facial capture, which refers generally to the quality of the image or footage. Additionally, it is often the case that digital images become 'degraded' through file conversion, scanning, as well as through the creation of passports or other documents that use watermark, etcetera; researchers are working to overcome this issue (Bourlai 2014). Facial obstructions are another central limitation as, perhaps obviously, the concealing of facial features literally hides information that the algorithms need to make a match. Glasses are often problematic here (although there has been progress in overcoming this), as well as 'excessive' facial hair; even a hat can be an issue depending on the placement of the camera. According to Bourlai (2014), the most common visual limitation is uncontrolled illumination, as individual faces can look very different under

varying degrees and angles of natural or artificial lighting – and FR software is particularly sensitive to this. Bourlai (2014) is a specialist in this area and is currently involved in a project which combines infrared cameras with FR technology in order to translate heat signatures into facial algorithms. This is part of a concerted effort for overcoming broader day/night illumination issues, as well as making FR software more feasible for future outdoor application. As opposed to 'night vision', infrared (heat signature) is more effective for FR software to identify individuals because cameras have a difficult time capturing the eyes of the subject in the dark – eyes are very important for the algorithm. As Bourlai (2014) explains, while thermal bands *cannot* detect eyes, thermal information can be translated to make a face and can detect *ears*; as such, much of the FR software currently in development is increasingly incorporating ear-shape into its algorithms.

While FR software continues to improve at a rapid pace, it still has *very* limited application outside of highly controlled environments. Additionally, even in the most disciplined settings, the success of FR software also depends on the size of the database. As Nalini Ratha (2014) – a biometrics specialist at IBM – notes: "as you increase the database, the error rate grows linearly". While airports have largely overcome this issue through maximizing user participation and through formatting passport photos to digitally accept the software, most other applications of FR technology rely on blacklists (such as terrorist watchlists, problem gamblers) and whitelists (such as employee lists, frequent flyers, voter identification). The accuracy of FR software, even under the best circumstances – in the lower 90%; while it might *appear* satisfactory, it is not reliable enough for facial biometrics to be applied on a "national scale", according to Loudermilk

(2014). In other words, using a national database is unfeasible at this point (and by contrast, DNA samples are up to 99.6% accurate (Loudermilk 2014)). This is why, as Jones (2014) of the DIA argues: "watchlists drive the intelligence community".

Despite all of the above limitations, local law enforcement and other entities continue to invest considerable time and money into FR software. One of the most recent and better-known uses of FR by law enforcement was its application following the Boston Marathon Bombings. Shortly after the two suspects had been identified through CCTV networks of various local businesses, Boston police and the FBI applied the technology on their captured faces, consisting of grainy video stills caught by the footage. The technology came up empty, even though both of the suspects' photos exist in official government databases and one of them on a FBI *watchlist*. The younger brother, Dzhokhar Tsarnaev had a Massachusetts driver's license; the two brothers had legally immigrated to the United States; and the older brother, Tamerlan Tsarnaev, had previously been the subject of an FBI investigation (Klontz and Jain 2013: 1). The failure of the technology was due to many of the previously discussed complications – particularly pose angle, facial obstruction, and image resolution. For example, probes for the younger brother, while still unsuccessful, exhibited notably better retrieval rates than probes for Tamerlan Tsarnaev, whose face was occluded by sunglasses (Klontz and Jain 2013: 5).

In another recent case, FR technology was utilized by the Vancouver police department to identify rioters following the aforementioned Vancouver Canucks' Stanley Cup loss in June 2011. As previously outlined in chapter 4.4, fans began photographing and posting thousands of pictures of the rioters on various websites and Facebook pages.

In the aftermath of the riots, the Insurance Corporation of British Columbia (ICBC) offered the use of its facial recognition software to assist police in identifying alleged vandals and rioters (Denham 2012: 2). The ICBC complied with various police requests and on at least one occasion, provided police with the possible identity of an individual; a disclosure that did not require a warrant or subpoena (Denham 2012: 25).

Both of the above examples are rather exceptional cases, however FR technology is gradually working its way into everyday policing. The software has its most extensive police-use in the United Kingdom, where it is credited with solving hundreds of crimes using developer Chris Solomon's 'electronic sketch artist' system. Solomon is a professor at the University of Kent and his software is used by 90% of British police and across more than thirty countries (Stenman 2013). Additionally, FR programs are emerging in numerous parts of the United States with the advent of mobile biometric tools carried by police, such as the Facial Recognition Pilot in Sand Diego and Chula Vista, California, and the Mobile Offender Recognition and Information System (MORIS) in Pinellas County, Florida (Loudermilk 2014). Deputies use the MORIS system to verify identities and bring up the criminal records of individuals such as people they have stopped who are not carrying other forms if ID, as well as accident victims and homeless people (Steel 2011). The Pinellas County sheriff's office claims (as of 2011) it has run thousands of identity searches this way since 2004, resulting in 700 arrests (Steel 2011). The MORIS system is capable of applying facial, iris and fingerprint recognition. Similarly in San Diego, police can use any tablet device programmed with FR software, to take a picture of an arrested individual and run it through their police computers; in an instant, the

system matches images taken in the field with databases of about 348,000 San Diego County arrestees (Winston 2013).

Most cases of contemporary police use of FR technology remain largely semi-automated and under controlled conditions, where the subject is often face-to-face with an officer. And while CCTV networks have sporadically been utilized in conjunction with FR software to assist in certain investigations, these cases still involve heavy officer supervision, in addition to a *specific* target. In other words, there is currently no known CCTV network that utilizes *automated* FR technology to police an urban space for law enforcement/crime prevention purposes. This is not to say however, that its implementation is not a future possibility, as numerous law enforcement and intelligence agencies have expressed a desire for such a system, and there has been experimental application throughout the West (see Gates 2011: 63-96). Funding for biometric police projects is also seeing a dramatic increase. For example, the Seattle Police Department will soon use facial recognition software to allow officers to compare photos captured by surveillance cameras with an existing database of 350,000 mug shots (Sanburn 2014). Seattle will become the nation's largest city to employ the emerging technology, and its use will be watched closely by other municipalities. The city is using a $1.6 million grant from the U.S. Department of Homeland Security to fund the program (Sanburn 2014). According to Seattle police, use of the software will be limited to people 'reasonably suspected' of criminal activity. The department has also agreed to track which officers will use the technology in order to prevent it from being deployed broadly. This factor has quelled some of the backlash from groups such as the American Civil Liberties Union (ACLU) (Sanburn 2014).

One of the only notable cases of (uncontrolled) automated FR systems being deployed throughout a CCTV network for 'preventative purposes' (otherwise known as smart CCTV) is the 2001 case of Ybor City in Tampa, Florida. In an effort to transform central Ybor City into a more desirable tourist and consumer destination, Tampa police installed a FR program called 'FaceIt' into thirty-six CCTV cameras across two blocks of its entertainment district (Gates 2011). Tech giant Visionics installed the system for free as the manufacturer promised that FR would help cut labour costs and facilitate commerce by making the space more secure through deterrence and the potential weeding out of '(un)wanted individuals' (Gates 2011). As Gates (2011) elaborates:

> Facial recognition technology promised to perform some of the labor of monitoring, *breaking through the anonymity of the crowd* to target select individuals. On a symbolic level, the publicity surrounding the facial recognition system was meant to convey the message that individuals would no longer be anonymous in the crowd, but instead would be individuated and identifiable (Gates 2011: 83, italics).

Controversy broke out immediately following the announcement of the program, with a wide range of voices emerging from the press, policy makers, the public and privacy organizations such as the ACLU – all with varying interests and interpretations of the technology (Gates 2011: 87). However, there was a surprising amount of support for the project, as the program's logic ran parallel with the crime control perspective that had been unfolding since the 1970's, through which "pitting the rights of 'the majority' against an essentialized class of criminals" fit with the growing public demand for stronger measures of punishment and protection (Gates 2011: 91). This also fit with the crime control initiatives of the criminal justice system as law enforcement officials were

eager to experiment with innovative new ways of *managing* crime (as opposed to assuming that crime could be reduced or potentially eliminated by addressing the social and structural conditions from which it is produced) (Gates 2011: 68). However, these arguments eventually became overwhelmed by the glaring inefficiency of the project, as Tampa police could not produce the success story that they so desperately needed to justify the invasiveness of the system and its potential cost. Subsequently, after a two-year free trial period, the Tampa police abandoned the effort to integrate automated FR with the Ybor City CCTV system in August 2003, citing its failure to identify a *single* wanted individual (a number of officers emphasized that the system's dismantling had little to do with privacy issues) (Gates 2011: 65, 94).

While the failure of the Ybor City Smart CCTV project may have set back automated FR from being depicted as a viable technology, it certainly did not spell the end of the attempt to integrate FR technology with video surveillance systems and law enforcement initiatives (Gates 2011: 95). This is evident from the myriad of FR projects that have been in development since the Ybor City experiment in 2001 - a number of which have been addressed in the preceding sections. Gates (2011) also emphasizes the experimental quality of the Ybor City Smart CCTV program, which she outlines as follows:

> . . .from the beginning, people directly involved in the project understood the highly experimental nature of what they were doing, and despite public statements about a smoothly functioning system, they were likely well aware that there was no guarantee the experiment would be successful (Gates 2011: 95).

As such, if we can say that the Ybor City experiment was useful for anything, it would be the unearthing of various social and technological issues and controversies that may arise from the future installation of a functional automated FR system. And since 2001, FR programs have not only proliferated across various institutions and sprung up in an increasing number of law enforcement agendas, but have emerged throughout various sectors of the commercial sphere as well. The commercialization of FR technology could mean a dramatic shift in user acceptance of FR software and its political relationship to surveillance, policing and security. This also raises important questions regarding consumer surveillance and the sharing of sensitive data, all of which boils down to the broader issues of data privacy and public anonymity. The following chapter explores these issues.

5.2 Consumer Transparency and Commercial Facial Recognition Technology

> I am seen (watched, noted, recorded) therefore I am (Bauman 2013: 130).
>
> Most crowds these days flow past scores of closed-circuit surveillance cameras as they move through the city – cameras that will likely one day soon develop the capacity to recognize individual faces and link them to personal information (Andrejevic 2007: 6).

Post-industrial institutions are increasingly defined by regulating procedures with 'very high rigidity and visibility'. The inspecting gaze of video surveillance places limits on contexts and circumstances of action as post-industrial citizens work to avoid drawing the attention of the camera – *appearing normal is what really counts* (Lianos 2012: 99, 102).

However, as discussed in section 3.2, Lianos (2012) places too much emphasis on social control's relationship to the homogeneity of the crowd which overlooks the enlarging culture of interactivity and circular feedback between the subject and the institution; a relationship that could lead to a potentially *more* potent form of social control. This phenomenon is related to the increasing transparency of the liberal subject in the information era and subsequently, through the dispersion of personal data throughout the private sector. The ceaseless efforts to make the anarchy of data flows *useful*, is demonstrative of a central theme of this essay, through which new kinds of visibility provide new avenues of exploitation, opportunities of governance, and new relationships of power and control – in a word, a new kind of imperialism. As this chapter argues, the bondage of identity to expansive pools of data, has bestowed post-industrial faciality with an unprecedented social weight, fostering a political climate through which FR technology could potentially flourish as a robust mechanism of social control. The future potential of facial recognition systems could be very problematic as the desire for corporations and the state to exploit consumer-citizen visibility will further and further alienate individuals from their own bodies, identities, and the *technology* used to identify them (Denham 2012: 12). Subsequently, the following chapter (5.3) addresses the issue of privacy and advances a critique of this concept, drawing from the anti-security arguments of Henry (2013) who posits that "privacy is in fact deployed as a means to structure the fields of relations through which security interventions are made" (Henry 2013: 95).

While the practices of identification have never been exclusively a state project (as it is always intertwined with the self's relationship to security and culture), much of

the social weight and organization of identity – in other words its liberal 'authentication' - has largely been concentrated in statist security politics, as much of this analysis has illustrated. However, the 'consumer turn' of the post-war era saw a relocation of some of this power into discourses of the business sector, such that official identity became increasingly codified by the consumer sphere; the 'financialization' of identity (or its 'securitization', to use Rose's language) is a notable turning point demonstrative of this trend (as discussed in section 4.3). For these reasons, it is widely accepted in contemporary surveillance literature that material identities are now *fragmented*; the solid frame of identification characteristic of modernity has become dissolved by the computerized corpus of liquid surveillance in post-industrialism. The quality of the post-industrial person is "relentlessly being stripped away as the self is endlessly divisible and reducible to data representations via the modern technologies of control" (Williams 2005 in Best 2010: 10). And subsequently, surveillance increasingly consists of data fragments which are generated, replicated and modified continuously (Best 2010: 20). William Bogard (2006) echoes very similar ideas:

> Societies of control. . .exercise power. . .[through] the radical deconstruction of the binary basis of identity. What matters most in [post-industrial] forms of control is the absolute fluidity of identity, the disappearance of the line between self and other, the seamless integration of bodies and information systems (Bogard 2006 cited in Haggerty & Ericson 2006: 64).

While Bogard (2006) is right to emphasize the fluidity of identity and the marriage of bodies and information, Bogard's argument - like Lianos' (2012) - overstates the blurring of 'self and other' in mechanisms of social control. As Andrejevic (2007) and other scholars (Gates (2011); Turow (2006); Tinic 2006) have argued rather convincingly, the

'permanent gaze' of post-industrial (liquid) surveillance is increasingly interested in overcoming the 'problem of the crowd' – in other words, piercing homogeneity – or 'hyper-regularity' to use Lianos' (2012) language – in order to extract unique variables related to identity in order to make consumer-subjects more productive and profitable. Examples used in the preceding section are illustrative of the concerted effort by the state to overcome the 'problem of the crowd'; and as Andrejevic (2007) argues, we must not underestimate the lengths with which *marketers* are willing to go 'to render consumers visible' (87). Consumerism continues to permeate the cultural fabric of the West and subsequently, market surveillance is becoming a burgeoning issue as companies are able to track our movements, transactions, and communications without our permission or, in many cases, knowledge (Andrejavic 2007: 4). Post-industrial digital technologies have introduced new avenues of exploitation through which fragments of consumer data become commodified. Essentially, identities are made *useful* for circulations of capital. As Bauman (2013) so aptly puts it: "*members of the society of consumers are themselves consumer commodities*, and it is the quality of being a consumer commodity that makes them bona fide members of that society" (33, italics in original). Participation throughout the market increasingly requires consumers to entrust their information to corporate entities as a condition of access and agency within commercial spheres of governance; much like the institutional structures through which consumer culture operates, a degree of control becomes a condition of access, privilege and freedom (Lianos 2012: 4, 6).

Some scholars have termed this process of exchange as 'customer relationship media' (CRM). Compliance and loyalty to the demands of CRM are rewarded with convenience, favourable access, social status and promises of security; however, these

benefits come at the escalating expense of privacy as individuals sacrifice their personal information and anonymity in order to partake in neoliberal culture and avoid being caught in an outmoded consumer base that may lead to alienation, exclusion, or simply, inconvenience. Facebook, digital video recorders (such as TiVo), customer loyalty programs and recurring software or interface updates are common examples of this. The phenomenon of CRM has proliferated throughout Western societies, changing how individuals experience media and culture, and has been referred to uncritically as a 'democratic new-media revolution'. However, some scholars approach the development more cautiously, referring to the trend as 'iculture' (emphasizing *interactivity* by the consumer-subject), and in some cases, as 'unpaid audience labour' (see Andrejevic 2007: 188-191). And while the practice of CRM often takes on the guise of a consensual agreement between consumer and business, the burgeoning influence of what Andrejevic (2007) terms 'iculture', fashions these decisions as rational calculations where concrete, immediate rewards are more culturally desirable than the unsung values of privacy and anonymity (see Best 2010: 21). While some have touted CRM as a 'win-win' form of consumer empowerment, Andrejevic (2007: 106) and Lester (2001: 28) have referred to this trend as the "tyranny of convenience", as not only is resistance to CRM constructed as irrational, but most consumers do not experience surveillance to be a process that targets 'whole populations' and individualized consumer interests (Best 2010: 20). CRM is problematic as it bestows businesses with state-like qualities to govern their consumer base; it can therefore be argued that corporations increasingly act as intelligence-gathering machines (Neocleous 2003: 49) which monitor, conduct and recruit. Andrejevic encapsulates this atmosphere quite well in the following passage:

> The question that we need to ask ourselves as we embark on the impending era of technologically facilitated 'relationship' marketing is not what marketers want to know about us, but whether there is any information they *don't* want to know about our lives. The answer, one suspects, is a resounding 'no' (Andrejevic 2007: 15).

Marketers are always looking for innovative new ways to monitor customers – especially in the security market (Andrejevic 2007: 91). As such, identification practices have become a central focus of CRM techniques and business models more generally. Recent developments in identification systems have seen an "intensified involvement of non-state actors as both suppliers and users of identification technologies" (Gates 2011: 34). As Gates (2011) elaborates:

> As the process of upgrading government ID systems was outsourced to private companies, and as the business sector made demands for more secure forms of government-issued identification, the respective roles of state versus private-sector actors in both the supply and demand for biometric technologies became increasingly difficult to disentangle (Gates 2011: 51).

While the state remains the largest buyer of FR software, the technology is applied sporadically throughout the Western commercial sphere, with the biggest private purchasers being casinos and banks. FR technology was marketed commercially to casinos as early as 1996, and in the US, a system was first installed at Trump Marina Casino in 1997. The software helped the casino nab eight baccarat cheats only three days after its installation. FR software continues to be used in casinos today, and sometimes in bars and clubs that house gambling, most often to combat cheaters and problem gamblers (Fisher 2013). In more exceptional circumstances, the technology has also been used by casinos to identify card counters. According to a representative from 'Aware Biometric

Software' (2014), in one instance, cameras were installed into a flashy advertisement which attracted the attention of casino clientele as they made their way down an escalator. This provided security officials with a 'head-on' image of every individual entering the casino, making it easier for FR technology to identify blacklisted individuals (to which security awaited at the bottom). The biometrics industry is also working with casinos in Japan to develop 'gambler loyalty programs' which involves personalized customer service opportunities (Ginovsky 2013).

The financial industry is another large commercial buyer of the technology, which in most cases, is using it as an additional layer of security to protect against identity theft and fraud. While most of these projects are still in the works in Canada, Europe and the US, a number of Asian, African and South American countries such as Kenya, South Africa, India and Japan have ATM machines that utilize FR technology to verify the identity of its users before a transaction can be made (some use iris scanning as well). Japan, for example, is one of the only advanced industrialized countries in the world that has been using biometric ATMs extensively for years. This is due to legislation that made banks liable for withdrawals made by criminals using stolen bank cards. In response to this, Japan now has over 80,000 biometric ATMs in service, used by more than an estimated 15 million customers (King 2012). If we recall, in countries such as Canada, the US and the UK, security is highly commodfied, constructed as an *individual* responsibility; as such, we can see how Japanese banking security stands in stark contrast to these nations, where individualized culture has arguably become intertwined with security mechanisms and policy. As a consequence, it may still be a number of years until other advanced-capitalist nations introduce biometric ATMs.

Facial Recognition and Consumer Relationship Media (Whitelists)

> We would find it unacceptable if a stranger would photograph our face for no apparent reason. On the other hand, we don't find it unacceptable to surrender our faces for the regulation of privileges – as long as we are in control of its use and circulation (Introna & Wood 2004: 178).

Aside from gambling and finance, FR software has emerged as a public technology throughout parts of the Western consumer sphere, in many cases transcending the technology's original role as purely an institutional security mechanism. Popular smart-phone applications such as 'Face Unlock' and 'Facevault', for example, provide personal security in the form of 'shrink-wrapped facial recognition technology' (Gates 2011: 138), allowing users to 'unlock' their Apple or Android phones via FR software that utilizes the phone's camera (see Bonnington 2012). Other phone applications utilize FR software for amusement or entertainment purposes, through which the technology distorts a digital image of the face (which can be taken from the phone's camera) for humorous effect. For example, 'Zombify' transforms the facial image to look like a zombie, 'Fatify' creates the illusion of weight gain, and 'Oldify' makes the user look older. Similarly, another application called 'GamePaint' allows users to submit their portrait to virtually paint their faces in their favorite NFL team colors. Parts of the beauty market are also using FR in very similar ways, albeit as a marketing tool. An example of this is 'VOGUE's Makeup Simulation' application, which recently launched in Japan. This app lets users try on makeup on their own photo (with facial detection and modeling being used to create a photorealistic rendering of the makeup on the user's image) (Aarabi 2013). Another example is Johnson & Johnson's 'ROC Skincare', which recently launched a 'Skin

Correxion Tool' to simulate the effects of their anti-aging products (Aarabi 2013). As Parham Aarabi (2013), CEO of ModiFace (a 'makeover app' that utilizes FR), posits:

> In the next few years, it would not be surprising to see interactive ads that use online photos to preview products (i.e., where each user is the model), or to recommend products based on the user's custom profile (Aarabi 2013).

Additionally, Hollywood and the video game industry have been increasingly invested in FR technology, through which it is used to fashion computer-generated (CGI) faces from the real faces of human actors. The technology was used extensively in the 2009 film *Avatar* and the 2011 video game *L.A. Noire*. In another instance, EA Sports - using a FR program called 'Game Face' - allows their users to upload images of their face through which the technology generates a computerized copy to be used in a variety of sports video game franchises. Other unique uses of FR software include a Google Chrome app for Youtube that utilizes webcams to determine whether or not a user is watching a video; the application pauses the video if the user looks away from the screen. One of the earliest usage of FR for advertising purposes was in a 2009 Coke Zero campaign through which users could submit their photo to find their doppelganger (assuming that a similar-looking person opted into the network as well). Additionally, viewers of the website could vote on how good the likeness was, helping to refine the system (Diaz 2013).

Importantly, while all of these examples certainly involve a form of FR software, it must be noted that their usage here either does *not involve connecting the individual to a database* (such as its application in films), or the database is personalized and involves a single individual (as in the case of the phone apps). As such, because in both instances the software is being *utilized by the observer*, this personalization and explicit consent by

the subject is likely why such programs have not experienced controversies over data privacy in the West. FR's relationship to consumerism becomes much more problematic when it escapes personalized use.

Since FR technology is marketed as a next-generation security mechanism, it is subsequently applied most frequently as an access management device or a policing tool for blacklisted individuals, by the state and private sector alike. However, a number of businesses are beginning to see facial biometrics' untapped potential to facilitate CRM initiatives. When utilized at a personal level (as in the preceding examples), facial recognition technology is often met enthusiastically and has largely flown under the privacy radar. However, controversy has recently been mounting following its application by social media websites and various cases of target marketing; processes which are more intimately involved with the subjects' identity and where consent is less explicit.

The potential of FR software in advertising campaigns has drawn the attention of marketers across the West. In one of the lesser intrusive examples, Douwe Egberts Coffee organized a promotion in which a vending machine was installed at Johannesburg's O.R. Tambo International Airport, equipped with FR technology. When a passerby would stare at the advertisement and yawn, the software would recognize the action and the machine would dispense a cup of coffee (the Youtube video of this recorded event has nearly half a million views) (Dicker 2013). It is likely that this campaign drew inspiration from similar – albeit more questionable – FR advertising efforts from parts of Asia. In Taiwan, South Korea and Japan, vending machines programmed with FR software are able to recognize unique variables of the face and offer, for example, hair-growing tonic to balding men or razors to people with beards

(Agence France-Presse 2010). This type of FR is also equipped to 'see' age and gender using a one of many programs called 'PanelDirector', an interactive advertising system that uses a small camera able to capture an image of anyone that looks at it. The individual's face is then compared to more than ten-thousand patterns stored in its database and the device is able to determine the gender and approximate age of the viewer (Ryall 2010). Armed with that information, the machine will suggest to a woman in her twenties, for example, a slightly sweeter beverage, based on the results of extensive market research; some machines may also display an advertisement appropriate to that person's assumed demographic. There are also some fashion outlets that have this technology mounted into the 'eyes' of their mannequins – such that they can literally 'look back' at viewing customers and gather information and/or project a tailored advertisement on a nearby screen. Lastly, shopping malls have also installed this software in mall billboards across parts of Asia, and the developers are looking to expand this service into North American countries (Ryall 2010)

While the laws regarding biometric surveillance in parts of Asia are more flexible than in the West, this more intrusive type of FR software is gradually making its way into Western marketing. In the UK for instance, supermarket giant Tesco will be installing FR software at checkouts and petrol stations this year (2014), under a five-year contract deal with developer Lord Sugar's Amscreen. Using technology very similar to its Asian counterparts, Tesco's FR system, which involves the strategic placement of screens, will identify the approximate age and gender of its clientele. This information will provide a tailored advertisement to the viewer, one that also adjusts depending on the time and date (such as Christmas), as well as on customer purchases at the time (Press Association

2013). It is also likely that meta-data will be created from these transactions, which may be relayed back to marketers for a more detailed look at Tesco's demographic (for example, young men tend to shop more at X time, older women at Y time). According to Tesco, the screens are projected to reach a weekly audience of more than five million adults; the company also maintains that the system does not store the images in a database (Press Association 2013). Walmart has also recently expressed interested in the software, albeit only for security purposes – for now (Strohm 2013).

Another Western case of commercial use of FR software – one more intimately connected to identification - is the 'Facedeals' phone application which is currently in development in parts of the US and Canada. Facedeals works with local businesses by installing marked 'Facedeal' cameras at the entrance of a partnered location, which proceeds to scan customers' faces. If said customer opts into the app on Facebook and verifies his or her photograph, then Facedeals messages their phones about good deals and promotions while shopping inside; the customer may also be notified of a *customized* deal based on their Facebook 'Like' history (Grey 2013). While the application is still in beta-testing, Facedeals CEO Dave McMullen says that the company is looking to launch in multiple locations by early to mid 2014 (Gesenhues 2014). The application is not officially affiliated with Facebook, however the social media giant has been experimenting with FR technology over the last few years, leading to one of the most controversial uses of the software.

In late 2010, Facebook launched a program called 'Tag Suggestions', which utilized automated FR software to suggest the names and profiles of people pictured in new photos that users uploaded to the site; it was first made available in the US and went

worldwide by June 2011. However, drawing controversy around privacy concerns – particularly in the UK - this feature was eventually removed (see Corbin 2012). However, Tag Suggestions resurfaced on Facebook in early 2013 in parts of the United States, allowing users to opt-in or out of the program under their 'privacy settings' (Butcher 2013). The technology is currently unavailable to Canadians as Facebook locked horns with Canada's privacy commission in 2009 after members of the Canadian Internet Policy and Public Interest Clinic (CIPPIC) at the University of Ottawa complained that the privacy information Facebook provides to users was confusing or incomplete (Elash 2012). Currently, the feature *does* appear on Canadian Facebook profiles under the 'Timeline and Tagging' settings, but reads: "this is not yet available to you".

5.3 A Critique of Privacy: Problematizing Facial Recognition Technology

Like the proliferation of photo identification and CCTV networks before it, FR is the next logical step in optic surveillance. The software is gaining momentum throughout the Western world as businesses and the state have begun to tap into its potential to capitalize on the exposed physical body and its bondage to the individual's digital counterpart. By placing facial identification at the mercy of this technology, FR software can simultaneously create and expose lucrative pools of data which can be exploited to maximize productivity and profit. While the software still has many challenges to overcome – especially for installment in uncontrolled conditions – facial algorithms are improving at a rapid pace, bolstered by institutional funding under a market which is

expected to triple in size (the global facial recognition market is estimated to grow from $1.92 billion in 2013 to $6.5 billion in 2018) (Jones 2014). As John Boyd (2014) of the DoD puts it: "the technology is not going away".

While the market demand for FR technology is expanding across the West, policy and privacy issues remain the most significant obstacle for the implementation of FR by the state and private sector alike. As Dalton Jones (2014) curiously puts it: "some countries view biometric data as defending privacy, we [the United States/the West,] view it as threatening privacy". For state officials such as Jones (DIA), Boyd (DoD) and Loudermilk (FBI), biometrics are viewed as an 'enhancement' of privacy due to their potential as a supplementary layer of security. For Loudermilk (2014): "biometrics protect privacy by positively identifying subjects, clearing those wrongfully accused". Strangely bypassing the traditional argument that security and liberty must be 'balanced' (see Neocleous 2007; Neocleous & Rigakos 2011), these narratives suggest that *privacy must be invaded to protect privacy*, which adheres to the one-dimensional logic of 'state as protector' that assumes an unwavering righteousness on part of the governing body. Also, Loudermilk's argument (2014) that biometrics protect privacy by clearing the wrongfully accused does not account for the fact that biometric technology (of whatever sort) also has the potential to *incorrectly* identify an individual. There is always the chance that the authority of forensic evidence may *secure* a wrongful conviction (recalling that DNA samples for example, can be "planted at crime scenes…mislabeled, badly filed, [and] inadvertently mixed or contaminated with DNA from elsewhere" (Tudge 2011: 99)). Corruption and misconduct on part of state actors are notably absent from these accounts.

This rationality is similar to the logic of CRM initiatives that involve biometrics for the protection of consumer data by a corporate entity, as more and more, customers are encouraged to relinquish personal information for additional security. Unlike state security however, consent to consumer FR is more explicit, the identities of subjects are not tied to official databases, and individuals who opt-in are *not suspect*, where under state control, the individual is always subject to scrutiny and possible intervention. Consumer applications of biometrics promise individuals a degree of control over these technologies rather than feeling controlled *by them* (Gates 2011: 136). In Finland for example, a company called Uniqul is launching a program this year that lets people pay their bills using their face – a program which is the first of its kind in the world. As a replacement for credit cards or cash, the subject stores their financial information under a Uniqul account (for a fee of course) and simply stares at a camera until it recognises them to make a payment (Vash 2013). Using 'military grade' algorithms, the subject's face takes from 0 to 30 seconds to be recognized. Uniqul is currently working with Paypal and marketing itself as a replacement for cashiers (as merchants must also invest in the software). Aside from this very new and experimental example, there is little evidence to suggest that this type of use of FR is gaining much momentum in the West, aside from the growing popularity of micro-level personal security mechanisms such as biometric phone apps. This might seem unusual at first, as this form of FR (for personal security) is arguably one of the lesser intrusive uses of the technology; however, its passivity in the consumer-security sphere is likely due to 1) FR software's very limited marketing as an enhancement for institutions equipped with CCTV networks; and 2) the fact that other biometrics - such as fingerprint scanning - are more reliable for personal consumer-

security use. This is not to say that FR software will not emerge as a viable identity-security mechanism, but under the current atmosphere of *individualized* security in the West, FR is largely impractical or unnecessary as a personal security technology. As such, the software will likely remain under the radar until businesses view it as a profitable enterprise (which may require a success story in a program such as Uniqul).

At the liberal policy level, the perceived dangers and controversies surrounding FR technology lie in its threat to personal privacy and anonymity through its application in the public sphere by both the state and the private sector. These issues are concerned with function creep and the opaque relationship between these two spheres, through which sensitive data can potentially be shared, leaked or bought and sold between companies and governments, and between different nation-states. As Elizabeth Denham – the British Columbia Information and Privacy Commissioner – explains, function creep occurs when a process or system "intended for one purpose is subsequently used for a new or originally unintended purpose. When personal information is involved, function creep implies that the change in use is without the knowledge or consent of the individuals" (12). When dealing with digital abstractions such as biometric algorithms and data flows, function creep is an extremely difficult thing to conceptualize, track and police, regardless of the existing legislation through which the data is governed. Because of this, function creep is largely inevitable (Andrejevic 2007: 125), particularly for a technology as new, covert, and as experimental as FR software, for which – for the most part - legal measures cannot keep up.

Across the West, various privacy groups and institutions have problematized the application of the technology in all of its forms, from electronic use by Facebook and

Google, to commercial application through target advertising, and of course, the use of FR software by nation-states (see Cavoukian and Marinelli 2010; Denham 2012; Federal Trade Commission 2012; Hall 2012). There appears to be a general concern among these groups that the growing use of facial recognition technology by private organizations and the state 'threatens to extinguish our right to anonymity' (Cavoukian and Marinelli 2010). And across the West, there are few legal safeguards currently in place to 'protect consumer privacy and security' (Federal Trade Commission 2012). Privacy issues regarding the protection of personal information by the private sector differs slightly by province, state, and country and it is beyond the scope of this paper to tediously outline these - generally minor - differences. In addition to this, privacy reports suffer from the monotony of a circular liberal logic, as these documents tend to be organized as follows: security mechanism B is problematic for A's security, therefore it is 'recommended' that institutions 'should not' do X and 'should never' do Y, which 'should ensure' security of Z. From the documents that I reviewed (which discuss FR in Canada, the US and the EU), the general consensus for "securing consumer privacy and anonymity" from the commercial application of FR software can be summarized as follows: introduce security measures which promote "responsible use of facial recognition technology" (Cavoukian and Marinelli 2010: 14; Federal Trade Commission 2012) by maximizing institutional transparency and "citizen's control over the collection, use and disclosure of his or her personal information" (Denham 2012). While these documents recognize that the technology *will* be abused, discussions of why we need facial recognition software at all are dismissed under the guise of enhancing security; and as such, these documents can be seen as not much more than vehicles for ushering in a *socially acceptable* form of FR

software under a framework that does not 'unduly limit' the so-called "benefits of the technology" (Hall 2012). In addition to this, there are a number of key assumptions underpinning the logic of these privacy reports. For example, the Information and Privacy Commissioner of Vancouver argues the following:

> Offering up [your facial biometrics] authorizes and enables others to use your body for purposes of their own. It thereby objectifies the body by isolating the physical element from the person and providing it as a means to an end in which the person has no inherent interest (Denham 2012: 11).

While there is certainly some truth in this passage, Denham (2012) does not consider that perhaps identification has *never* operated in 'our interest'. Identification is precisely about using and *seeing* the body for the purposes of institutional interests. Therefore, it is problematic for these reports to suggest that Westerners 'reclaim control over' their identities, as *identification itself is a form of control*, and FR is an extension of its optic reach. The Information and Privacy Commissioner of Ontario even evokes the Orwellian dialogue (used also by FBI's Loudermilk (2014)) to suggest that FR surveillance technology can be used to "protect privacy rather than encroach upon it" (Cavoukian and Marinelli 2010: 5). In her report, Cavoukian (2012) - in collaboration with Tom Marinelli, the Chief Information Officer of the Ontario Lottery and Gaming Corporation - advocates a 'privacy by design' approach, a so-called "win-win" situation (for who?) that utilizes 'simple FR' "without compromising functionality, security or performance" (1). "Promising" to be applied only to problem gamblers, this program shares the logic of something like 'safety by design' for the production of firearms.

Governed by more a clear set of laws regarding the protection of 'personal information', facial recognition software's relationship to the state differs from its application in the commercial sphere, even though it is largely handled in the same way by liberal privacy groups who advocate policy measures that emphasize personal data security and institutional transparency. In the US for example, the Constitution only covers individuals from privacy intrusions by the state (not the private sector), providing *some* 'protections' for potential misuse of FR technology by government institutions (although policing this, as we will see, is largely impossible). For example, US police may have the right to ask a person their name, but there is currently no basis for them to seize an individual's official identity – a standard which will become complicated by the surreptitious nature of FR software. Conscious of legal obstacles, Boyd (2014) of the DoD asserts that the implementation of "facial recognition technology is technically straightforward, but not policy wise"; and similarly, Jones (DIA) (2014) posits that the use of biometrics by the state "revolves around laws and policies", and that "this is a very complex problem that no one can wrap their head around". Arguably, the most significant obstacle policy-wise is the sharing of biometric information between state departments and private/public institutions, (and to a lesser extent, internationally). The national security complex, reinforced by the legal ambiguities of globalization have made sharing among the international community a more streamlined process than interstate efforts, as the "majority of nations have national security of public safety expectations that enable sharing" of biometric information (Jones 2014). INTERPOL, an international organization that cooperates with partnered countries in 'solving international crime' (from theft to terrorism) and identifying criminals at borders, has been a significant

player in this field, as the agency has operated as a central hub for the sharing and exchanging of biometric information across countries (funded by 53 'member countries' as of February 2014). While INTERPOL has utilized only fingerprints to carry out these functions (with a database of over 183, 493 prints), the agency recently signed a partnership with Safran Morpho in 2012 to develop a FR system called 'Morphoface', which will be implemented toward the end of 2014 (Branchflower 2014).

The sharing of biometric information becomes more difficult at the local/state level; as for example, in the US, there are currently five states where public and private institutions are legally prohibited to share biometric information with the FBI when it is conducting an investigation (see ***figure 3***) (Loudermilk 2014). Additionally inter-department sharing is particularly complicated and inconsistent, as for instance, the US Department of Defence cannot share biometric information with the Department of Homeland Security, but has an agreement to share with the Department of Justice (DoJ – which includes the FBI) (their databases are conjoined) (United State Government Accountability Office 2011). That being said, it is currently the case that most state-level biometric databases and watchlists are sporadic and disconnected from one another, even though biometric data only needs to be replicated once to be shared with other agencies (S. Lyon 2014). The problematization of this issue was particularly notable at the Biometrics for Government and National Security summit, as the state officials who made presentations emphasized that sharing information across all levels has become a central "strategic priority" for each state department (Loudermilk 2014; Jones 2014; Branchflower 2014; Boyd 2014). In Jones (2014) words: "we must work through the

legal issues" as "identifying individuals requires the seamless collection, storage, sharing and analysis of identity information".

As of now there is little in place to stop or slow the sharing of biometric information among and between states and the private sector, especially since the development and future of biometric technologies are dependent on a healthy relationship between business and the state. The Snowden-NSA revelations, while having little to do with biometrics (so far), are nevertheless particularly demonstrative of the limits of liberal privacy initiatives and the demands for government and institutional transparency. For example, one of the leaked NSA documents discusses the Toronto G20 summit of 2010, revealing that the US embassy in Ottawa became a nexus for G20 spying operations for the NSA; presumably to overcome the legal issues inherent in having Communications Security Establishment Canada (CSEC) spy on Canadian citizens (20131202-CBC-G20 2014). Additionally, the FBI has recently been sued by the Electronic Privacy Information Centre (EPIC) for not disclosing a single document regarding their 1.2 billion dollar Next Generation Identification (NGI) program spearheaded by private contractors such as Lockheed Martin and IBM (Vrankulj 2013). When completed, the NGI will be the largest biometric database in the world, encompassing fingerprints, palm prints, iris scans, DNA profiles, voice identification, and digital photographs (McCall, Rotenburg & Brody 2013: 3). According to EPIC, the vast majority of records contained in the NGI database will be of US citizens and will include photographs of individuals who were unaware that their images were captured, in addition to other biometric identifiers that have been collected without the explicit consent of the subject (McCall, Rotenburg & Brody 2013: 2, 3). The document also

suggests that the NGI database will be used in conjunction with the MORIS program – the aforementioned project involving portable devices in use by local law enforcement to identify suspects through their biometrics (McCall, Rotenburg & Brody 2013: 4). Thus, by taking security for granted, liberal privacy initiatives do little more than communicate the 'acceptable' limits of security projects, and offer an illusion of control by the individual – in the case of FR software, the fiction that identification regimes have been forged in our own interest (Henry 2013: 95, 104). For these reasons, privacy is a form of pacification, as it can ever only be articulated as something which defends *private life*, a concept championed by liberals which keeps "individuals apart and disinterested" and "restricts their capacity for rebellion" (Henry 2013: 100). Thus, even in the best case scenario - if a competent privacy policy recommendation becomes successfully incorporated into law – at the end of the day, we all return to the pursuit of private interests, with the 'egoistic individual' remaining fully intact (103). Henry (2013) puts it best in the following excerpt:

> security decrees the activities and relations that can be declared to form the individual's privacy. . .[thus,] the success of privacy, its very completion, offers nothing more than a return to the freedoms of private life, which is a return to the freedoms that conditioned and deployed the apparatus of security in the first instance (Henry 2013: 103, 104).

As such, it is not enough to challenge FR software from a privacy perspective as, like all police projects, the technology is but an extension of social imperialism that will further cement existing inequalities. The following section explores these issues, and chapter 6 concludes with a discussion about resistance.

The Death of Anonymity? Not Really: Problematizing the Exposing Gaze

Andrejevic (2007) captures quite vividly the essence of 'smart' technologies in the following passage:

> Technology promises to reanimate the world – this time with the intentionality of humans rather than that of the spirit world. Instead of river sprites and wood nymphs, we will have appliance animism: devices that talk to one another, buildings that recognize us, and rooms that adjust the climate, music, and lighting to fit out preferences – or perhaps to shape our moods (based on biometric feedback) (Andrejevic 2007: 122).

It is not difficult to imagine a future where shopping malls and supermarkets 'know' us down to the finest details, from our preferred forms of entertainment, restaurants and clothing, to our address, finances, politics and diet; a future where we can scan our bodies to pay for items and services or gain access to concerts, amusement parks and clubs; and a future that promises safety and security from 'risky' outsiders. This is also a future of exposure, where our digital nakedness is subject to seamless and sophisticated scrutiny, where deviances are either opportunities for marketing or flagged as risks for the security apparatus; and it is a future where the substance of our lives are defined by and thus, *dependent on* institutions and their structured relationships.

Finally, this is a future where the poorest of us - unable to network or access such technologies - are excluded from the perks of the institutional world, as the inability to 'stand out' in the information economy is to be worthless to the system and its culture. As Lianos (2012) puts it: "individual identity will not use means to constitute itself that cannot be cashed at the social stock exchange" (113). And lastly, in this future, blemishes

on one's identification (such as a criminal record) become magnified as a defining feature of the person, which is especially problematic for the poor, who may be unable to express themselves any other way. Thus, if we use Andrejevic's language and say that smart technologies are 'reanimating the world' with the 'intentionality of humans', it most certainly is a world carved from those who benefit most from the inequalities of neoliberal capitalism, and therefore, the future envisioned here is little more than an intensification of the processes which define bourgeois society.

As such, the problem is *not* that FR software will potentially put an "end" to anonymity - as liberal privacy advocates claim (OPC Research Reports 2013: 12; Denham 2012: 11; Danzico 2011; The Economist 2011; Cavoukian and Marinelli 2010) - but rather, that it will deepen discriminatory practices which are already in place by depoliticizing the inequalities inherent in identification practices and the material gaze of security. Firstly, to argue that FR software threatens anonymity in the public sphere is to suggest that there was once a time when Western subjects could move through public spaces anonymously to begin with. This is not to say such a time never existed, however, it is unreasonable to conclude that FR software single-handedly puts an end to this privilege. If one wants to draw these kinds of simple historical lines, it can easily be argued that anonymity has been deteriorating since the day the state imposed identification documents upon its subject population – or to go back even further, since the birth of taxes. Furthermore, the financialization and monetization of identity through the creation of meta-data from economic transactions in the 1960s and 1970s, is arguably a much more drastic step in extinguishing anonymity than the introduction of any sort of biometric technology. FR software is but an extension of these processes. It is an *enabler*

of *transparency* of the citizenry, something which the state has arguably always desired and always seeks to maximize. Thus, the idea that FR technology puts an "end to anonymity", illuminates how identification itself is a form of pacification, as to reiterate, liberal logic assumes that official identities are generated and expressed under conditions of our own choosing; and subsequently, the creeping of the state into our everyday lives becomes reduced to the language of security and privacy, depoliticizing the fact that *identification is the antithesis of anonymity*. Therefore, FR software should *not* be problematized as the 'death of anonymity', as firstly, it incorrectly suggests that Western subjects could live anonymously prior to the introduction of this technology (downplaying previous invasions of anonymity); and secondly, it does not take into account that there will *always* be visibilities to exploit. The 'death of anonymity' suggests that somehow, facial recognition software marks the 'end' of technologies exploiting our visibility (while infrared cameras and insect-sized drones come to mind).

Chapter 6: Conclusions

6.0 Reclaiming Visual Sovereignty: Resisting Facial Recognition Technology

> Just as the capitalist system continuously produces and reproduces itself economically on higher levels, the structure of reification progressively sinks more deeply, more fatefully, and more definitively into the consciousness of Man [sic] (Lukács 1971; orig. 1923: p. 93).

The intention of the preceding argument is *not* to make light of the invasiveness of FR technology, but rather to begin to problematize the software in a way that transcends the

hegemony of privacy politics – a perspective that has dominated discussions of the technology and the way we think about identity's relationship to biometrics (a relationship which is often taken for granted and rarely problematized). Instead, criticism of FR software (and biometrics more generally) must be directed at capitalism's colonization of the body – as the demand for this technology by the state and private sector marks, at the very least, a *desire* to 'read' crime and deviance from the body – and discriminate accordingly. To construct 'biological data as a means of social identification' (Aas 2011: 147) is to inscribe upon the body an interiority which is fixed, essential, bounded, asocial and ahistorical (Rimke 2003: 247), which – following the trends that characterize the culture of control - ignores the unequal relationships that people have to systems and structure. Subsequently, the discrimination inherent in policing and security (as well as marketing techniques) becomes articulated through the identification process of the software, which – unquestioned by liberal ideology - enjoys the appearance of political neutrality. This depoliticizes discrimination based on inequality and recasts these practices into rational calculations in the name of security. Andrejevic (2007) captures the essence of this phenomenon in the following passage, where he discusses 'weblining', which refers to the practice of denying certain opportunities to people due to observations about their digital selves (Collins Dictionary.com):

> [weblining] enables discrimination practices that are more opaque and harder to target because the decisions are made according to complex algorithms that may disguise the role that, for example, race plays as a basis for discrimination (Andrejevic 2007: 128).

While the social dimension of ethnicity is irrelevant to the mechanical processing of facial algorithms, it is not unreasonable to suggest that FR's role as a security mechanism will disproportionately affect people of colour and the poor as it enhances and streamlines surveillance systems already in place. The FBI terrorist watchlist for example, is composed nearly exclusively of Arab men. For the (US) military, as of 2011, one in twenty people in Afghanistan is registered in biometric databases (one in six men "of fighting age") and one in fourteen people in Iraq (one in four men "of fighting age") (Shanker 2011). Also, law enforcement, airports and borders are interested in using FR to keep a watchful eye for undocumented immigrants (Ganeva 2011); businesses can compose blacklists of undesirable clientele, such as loiterers and the homeless; and police will use the technology (MORIS program) to expedite the identification process, arguably providing them with more incentive to pull people over, increasing the likelihood of racial profiling. Also, it would be unsurprising to see FR systems marketed in the future as a tool for *combatting* racial profiling and other types of profiling – by replacing the gaze of imperfect (prejudiced) personnel with a 'neutral' technological gaze (de-racializing inherently racist and classist systems and structures).

Other notable groups that will be an early target of FR security initiatives are dissidents and protestors. This is evident in the way it has been used to identify individuals (often with the help of the public and media) in incidents such as the Vancouver Stanley Cup Riots and London's 2012 Games. Additionally, the FBI has shown interest in applying FR technology at political rallies (Bruegge 2010), and the software was used to identify individuals who participated in the Occupy Wall Street protests in Phoenix, Arizona (Hodai 2013). In the latter case, intelligence analyst Brenda

Dowhan was employed by the Arizona Counter Terrorism Information Center (ACTIC) and the Phoenix police to infiltrate the movement, from which she attempted to identify individuals believed to be associated with OWS through the application of FR technology to photographs of citizens found on Facebook (Hodai 2013). A document from the Center for Media and Democracy (CMD) reports the following:

> . . .the ACTIC Facial Recognition Unit, operated by the Maricopa County Sheriff's Office (MCSO), has the ability to match biometric data contained in photographs-- such as those found on Facebook . . .with biometric data contained in roughly 18 million Arizona Driver's License photos, 4.7 million Arizona county/municipal jail "booking" photos, 12,000 photos contained in the "Arizona Sex Offender Database," and 2 million photos available through the Federal Joint Automated Booking System (Hodai 2013: 27).

This information was gathered from a freedom of information laws request filed by the CMD, and it would be naïve to think that this is the only instance of FR software being used in this way.

Also significant are the anti-mask laws that have been introduced throughout the Western world. While this legislation obviously differs from country to country in circumstantial details and punishment, all of these laws concern the concealing of faces at demonstrations, protests, or riots. Countries that enforce such legislation include Canada, France, Austria, Denmark, Germany, Switzerland, Spain, Sweden, Ukraine, and parts of the United States; and in most of these cases, anti-mask law has been introduced in the last ten years. Canada is one of the most recent enforcers of this, amending section 65(1) of criminal code with Bill C-309's *Preventing Persons from Concealing Their Identity during Riots and Unlawful Assemblies Act*, which is outlined as follows:

> Every person who commits an offence under subsection (1) while wearing a mask or other disguise to conceal their identity without lawful excuse is guilty of an indictable offence and liable to imprisonment for a term not exceeding 10 years (Criminal Code 2014).

Additionally, Canadian law is rather vague in describing what separates a 'peaceful protest' from an 'unlawful assembly' (a distinction presumably made by the police). Given royal assent in summer of 2013, no one has, as of yet, been charged under Bill C-309. By contrast, New York State evoked a 150 year-old law to arrest members of OWS when protesters began to dawn Guy Fawkes masks as a symbol of resistance and collective anonymity. New York's Penal Law 240.35(4) makes it a crime for three or more people to congregate in public in a mask, unless it is "in connection with a masquerade party or like entertainment". Most recently, the law has been used to charge a small number of individuals who protested in 2012, demonstrating solidarity with the feminist punk protest band Pussy Riot, whose members had recently been jailed in Moscow. Like the band, a number of protestors wore brightly coloured ski masks to show solidarity with the group.

The practice of concealing one's face at a protest has been described as 'mummery', which refers to "all practices to conceal one's identity – usually by (partially) covering the face" (Haunss, forthcoming: 1). With the exception of the early 20th century Ku Klux Klan, mummery was highly uncommon at Western protests until the 1970s and 1980s with the introduction of video surveillance equipment by the police, where protestors began masking-up to avoid having their photographs published in newspapers - and later, uploaded to the Internet - causing personal or professional problems (Haunss, forthcoming: 3). Also, some forms of mummery (such as kerchiefs)

can be seen as a response to police use of chemical-based weapons such as pepper spray and tear gas. However, 'masking up' often means *more* than protection from social and legal consequences, as mummery itself can serve as a potent political statement (see Shantz 2003; Avery-Natale 2010; Haunss, forthcoming). Because protests and demonstrations are a spectacle, masks provide an outlet for *visual* forms of resistance and expression, ones that often defy the material basis of official identity and faciality by challenging individualism and emphasizing collective identity. One of the most intriguing accounts of this symbolism is the black bloc tactic, a method of anarchist protest which involves 'an erasure of identification', where the black mask supplants the old subject and represents the new subject (Avery-Natale 2010: 102, 104); the singular identity associated with the liberal face becomes eradicated – at once the anarchist 'becomes everyone' (Avery-Natale 2011: 103). Similarly, the leader/spokesperson of the Zapatistas, a revolutionary group based in Chiapas, dawns a black balaclava to hide his individual identity and communicate a message of collectivism, which Klein captures quite well in the following passage:

> Marcos, the quintessential anti-leader, insists that his black mask is a mirror, so that Marcos is gay in San Francisco, black in South Africa, an Asian in Europe, a Chicano in San Ysidro, an anarchist in Spain, a Palestinian in Israel, a Mayan Indian in the streets of San Cristobal, a Jew in Germany, a Gypsy in Poland, a Mohawk in Quebec, a pacifist in Bosnia, a single woman on the metro at 10 p.m., a peasant without land, a gang member in the slums, an unemployed worker, an unhappy student and, of course, a Zapatista in the mountains (Klein 2002).

Therefore, not only does mummery thwart the material gaze of the state (through FR software or otherwise), but it doubles as a type of resistance that refuses dominant forms of political representation. For these reasons, the push for anti-mask legislation is

disconcerting as the practice of mummery must be viewed as a fundamental part of political expression and free speech. The successful implementation of these laws is further demonstrative of how *facial identification is pacification*, as privacy advocates and liberal politics have failed to protect a mode of political expression that resists and transcends state narratives of identity.

This thesis has shown how the face's bondage to security has played a key role in the reification of modern subjects, specifically in the expression of identity and in the optic perception of the human body. FR software is but an extension of this historical process as the booming market of biometric technologies signifies the commodification of the body, and further cements its relationship to identification, and thus to the policing powers of security. Therefore, it can be concluded that facial identification – manifested as FR technology or otherwise - is a form of pacification because it attempts to neutralize struggles over identity and visual sovereignty. As a non-negotiable part of the human contract, facial identification seeks to place limits on political representation and subsequently, how resistance can be articulated. The discourse of privacy, perceived as the only way to challenge FR software, is demonstrative of this trend – as opposition can only be legitimately expressed through referencing back to the body's role as a productive enterprise (ie: how do we introduce a 'socially acceptable' version of FR software) all the while assuming its taken-for-grantedness within the logics of liberal capitalism. Instead, facial recognition technology must be resisted at the level of identification, as the boundaries enforced by this social sorting mechanism (one that becomes internalized through dominant cultural representations) increasingly strips Western subjects of their right to self-construction and political representation. The

starting point of any discussion regarding the invasiveness of FR software must therefore begin by exposing and dismantling the tendency for humanity to be reduced to codes and categories that satisfy capitalist production and consumption.

Bibliography

20131202-CBC-G20 (2013) "(S//REL) NSA Lends Support to Upcoming G8 and G20 Summits in Canada". Retrieved April 11th, 2014 via: https://www.eff.org/files/2013/12/02/20131202-cbc-g20.pdf

Aarabi, P. (2013) "How Brands are Using Facial Recognition to Transform Marketing". *Venture Beat*. Retrieved April 4th, 2014 via: http://venturebeat.com/2013/04/13/marketing-facial-recognition/

Aas, K., F. (2006) "'The Body Does Not Lie': Identity and Trust in Technoculture". Crime Media Culture. Vol. 2. pp. 143.

Abel, M., H., Watters, H. (2005) "Attributions of Guilt and Punishment as Functions of Physical Attractiveness and Smiling". *The Journal of Social Psychology.* Vol. 145 (6). pp. 687-702.

Ackerman, S. (2014) "US Tech Giants Knew of NSA Data Collection, Agency's Top Lawyer Insists". *The Guardian.* Retrieved April 11th, 2014 via: http://www.theguardian.com/world/2014/mar/19/us-tech-giants-knew-nsa-data-collection-rajesh-de

Agence France-Presse (2010) "Taiwan Develops Face-Recognising Vending Machine. *Phys.org.* Retrieved April 11th, 2014 via: http://phys.org/news/2011-01-taiwan-face-recognising-vending-machine.html

Andrejevic, M. (2007) *iSpy: Surveillance and Power in the Interactive Era*. Lawrence, Kansas: University Press of Kansas.

Associated Press (2001) "Smile! You're On Casino Camera". CBS News.com. Retrieved April 11th, 2014 via: http://www.cbsnews.com/news/smile-youre-on-casinocamera/

Banksy (2006) *Wall and Peace.* Century.

Bantjes, R. (2005) *Improved Earth: Prairie Space as Modern Artefact, 1869-1944*. Toronto. Toronto University Press. 2005.

Bauman, Z. (2001) *The Individualized Society*. Cambridge, UR. Polity Press.

Bauman (2004) *Europe.* Cambridge: Polity Press.

Bauman, Z., Lyon, D. (2013) *Liquid Surveillance.* Cambridge: Polity Press.

Beck, U. (1992) *Risk Society: Towards a New Modernity.* SAGE.

Beresford, A., D. (2003) "Foucault's Theory of Governance and Deterrence of Internet Fraud". *Administration and Society.* Vol. 35. pp. 82.

Berry, D., S., Zebrowitz-McArthur, L. (1988) "What's in a Face?: Facial Maturity and the Attribution of Legal Responsibility". *Personality and Social Psychology Bulletin.* Vol. 14. pp. 23-33.

Best, K. (2010) "Living in the Control Society: Surveillance, Users and Digital Screens Technologies". *International Journal of Cultural Studies.* Vol. 13. pp. 5.

Bogard, W. (1996) *The Simulation of Surveillance: Hypercontrol in Telematic Societies*. Cambridge: Cambridge University Press.

Bogard, W. (2006) "Welcome to the Society of Control: The Simulation of Surveillance Revisited". Chapter 3, In Haggerty, K., Ericson, R., V. (eds.) (2006) *The New Politics of Surveillance and Visibility*. Toronto: University of Toronto Press. pp. 55-78.

Bohmer, I. (2014, February) *Identity Federation Governance Managing Secure Authentication Across Trust Domains*. Presented at Biometrics for Government and National Security, Walter E. Washington Convention Center, Washington, District of Columbia.

Bonnington, C. (2012) "FaceVault App Brings Facial Recognition Unlocking to iOS". *Wired.* Retrieved April 16th, 2014 via: http://www.wired.com/2012/04/facevault-app-face-recognition/

Boyd, J. (2014, February) *Biometrics: A Department of Defence Perspective.* Presented at Biometrics for Government and National Security, Walter E. Washington Convention Center, Washington, District of Columbia.

Bruegge, R., W., V. (2010) "Facial Recognition and Identification Initiatives". Federal Bureau of Investigation Biometrics Center of Excellence. Retrieved from the *Electron Frontier Foundation* Aril 16th, 2014 via: https://www.eff.org/document/fbi-facial-recognition-initiatives-presentation-2010-biometrics-conference

Bohmer, I. (2014, February) *Identity Federation Governance.* Presented at Biometrics for Government and National Security, Walter E. Washington Convention Center, Washington, District of Columbia.

Bourlai, T. (2014, February) *Mobility and Biometric Smart Cards.* Presented at Biometrics for Government and National Security, Walter E. Washington Convention Center, Washington, District of Columbia.

Branchflower, M. (2014, February) *International Perspective.* Presented at Biometrics for Government and National Security, Walter E. Washington Convention Center, Washington, District of Columbia.

Bucknill, J., C., Tuke, D., H. (1858) *A Manual of Psychological Medicine.* Philadelphia: Blanchard and Lea.

Butcher, M. (2013) "Facebook Turns Photo Tag Suggestions Back On In The US — Will Users \ Like It This Time?". *Tech Crunch.* Retrieved April 16th, 2014 via: http://techcrunch.com/2013/02/01/facebook-turns-photo-tag-suggestions-back-on-in-the-us-will-users-like-it-this-time/

Butler, J. (1993) *Bodies that Matter.* London: Routledge.

Castel, R. (1991) "From Dangerousness to Risk". In Burchell, G., Gordon, C. & Miller, P. (Eds.) *The Foucault Effect: Studies in Governmentality*. Hampstead, Harvester Wheatsheaf: Hemel.

Cavoukian, A., Marinelli, T. (2010) "Privacy-Protective Facial Recognition: Biometric Encryption Proof of Concept". *Privacy by Design.ca*.

Chachere, V. (2001) "Biometrics Used to Detect Criminals at Super Bowl". *abc news.* Retrieved April 16th, 2014 via: http://abcnews.go.com/Technology/story?id=98871

Clemente, F., Kleiman, M. (1976) "Fear of Crime Amongst the Aged". *Gerontologist.* Vol. 16(3). pp. 207-210.

CNN Wire Staff (2011) "Osama Bin Laden, the Face of Terror, Killed in Pakistan". *CNN World.* Retrieved April 16th, 2014 via: http://www.cnn.com/2011/WORLD/asiapcf/05/01/bin.laden.obit/

Cole, O. (2014) "Hunger Games and the Limits of White Imagination". *Huffington Post: Entertainment.* Retrieved April 16th, 2014 via: http://www.huffingtonpost.com/olivia-cole/catching-fire-beetee-race_b_4334585.html

Connolly, J. (1858) "Physiognomy of Insanity: Insanity Supervening on Habits of Intemperance". *Medical Times and Gazette.* pp. 651-653.

Corbin, K. (2012) "Facebook's Facial Recognition Policies Draws Senate's Attention". *CIO.* Retrieved April 16th, 2014 via: http://www.cio.com/article/711505/Facebook_s_Facial_Recognition_Policies_Draws_Senate_s_Attention

Cosgrove-Mather, B. (2004) "Biometric IDs Gain Foothold". *CBS News*. Retrieved April 11th, 2014 via: http://www.cbsnews.com/news/biometric-ids-gain-foothold/

Criminal Code, R.S., c. C-46 (2014) *Preventing Persons from Concealing Their Identity During Riots and Unlawful Assemblies Act*. Retrieved April 11th, 2014 via: http://www.parl.gc.ca/HousePublications/Publication.aspx?Language=E&Mode=1&DocId=6246507&File=24#1

Crompton, J., C. (2013) "Bio-What? Biometrics. What It Is and Why It Matters". *SAP Business Innovation.* Retrieved April 11th, 2014 via: http://blogs.sap.com/innovation/industries/bio-what-biometrics-what-it-is-and-why-it-matters-0360446

Cumberbatch, G. (1988) "The Incidence and Nature of Violence in Television". In *Violence and the Media: Papers Presented to a Seminar Held by the BBC on 2nd December 1987.* BBC.

Daily Mail Reporter (2011) "Incredible Pictures Show President and Inner Circle Watching Live TV Feed as Special Forces Shoot Dead the World's Most Wanted Man". *Mail Online.* Retrieved April 14th, 2014 via: http://www.dailymail.co.uk/news/article-1382649/Osama-bin-Laden-dead-Photo-Obama-watching-special-forces-shoot-him.html

Deleuze, G., Guatarri, F. (1987) *A Thousand Plateaus: Capitalism and Schizophrenia*. Massumi, B. (trans.). Minneapolis, London: University of Minnesota Press.

Denham, E. (2012) "Investigation into the use of Facial Recognition Technology by the Insurance Corporation of British Columbia". *Office of the Information and Privacy Commissioner of British Columbia.* Investigative Report F12-01. B.C.I.P.C.D. No. 5.

Department of Army (2014, March 31) "Army Regulation 670–1: Uniform and Insignia: Wear and Appearance of Army Uniforms and Insignia". Department of Army Headquarters, Washington DC. Retrieved April 11th, 2014 via: http://armypubs.army.mil/epubs/pdf/r670_1.pdf

Diaz, A. (2013) "Facial Recognition Technology Makes Marketers a Fun Big Brother". *Advertising Age.* Retrieved April 11th, 2014 via: http://adage.com/article/news/brands-facial-recognition-campaigns/244233/

Dicker, R. (2013) "Machine Dispenses Free Coffee When You Yawn; Douwe Egberts Gizmo Works On Facial Recognition". *Huffington Post*. Retrieved April 11th, 2014 via: http://www.huffingtonpost.com/2013/07/19/coffee-machine-yawn_n_3623787.html

Dupont, D., Pearce, F. (2001) "Foucault Contra Foucault: Rereading the 'Governmentality' Papers". *Theoretical Criminology*. Vol. 5. pp. 123-158.

The Economist (2011) "Anonymous No More". *The Economist.* Retrieved April 16th, 2014 via: http://www.economist.com/node/21524829

Edkins, J. (1999) *Postrstucturalism & International Relations: Bringing the Political Back In.* Boulder CO: Lynne Reinner Publishers Inc.

Elash, A. (2013) "Facebook Facial-Recognition Feature Won't be Available to Canadians". *The Globe and Mail.* Retrieved April 16th, 2014 via: http://www.theglobeandmail.com/news/national/facebook-facial-recognition-feature-wont-be-available-to canadians/article588390/

Ericson, R. (1998) "How Journalists Visualize Fact". *Annals,* AAPSS, Vol. 560. pp. 83-95.

Evans, B. (2010). "Foucault's Legacy: Security, War and Violence in the 21st Century". Security Dialogue. Vol. 41: 413.

Fairclough, N., Wodak, R. (1997) "Critical Discourse Analysis" in Dijk, T. (ed.) (1997) *Discourse as Social Interaction*. London: Sage. pp. 258.

Faronni, T., Menon, E., Rigato, S., Johnson, M., H. (2007) "The Perception of Facial Expressions in Newborns". *European Journal of Developmental Psychology*. Vol. 4. pp. 2-13.

fbi.gov (2014) "Most Wanted Terrorists". *The FBI: Federal Bureau of Investigation.* Retrieved April 16th, 2014 via: http://www.fbi.gov/wanted/wanted_terrorists

Ferguson, C. (2007) "Eugenics and the Afterlife: Lombroso, Doyle, and the Spritualist Purification of the Race". *Journal of Victorian Culture*. Vol. 12 (1). pp. 64-85.

Fink, B., Neave, N., Manning, J., T., Grammar, K. (2006) "Facial Symmetry and Judgements of Attractiveness, Health and Personality". *Personality and Individual Differences*. Vol. 41 pp. 491–499.

Foucault, M. (1971) "Neitzshce, Genealogy, History" in J. Faubion (ed) *Essential works of Michel Foucault 1954-1984*, Vol. 2

Foucault, M. (1972) *Archeology of Knowledge.* London: Tavistock Publications.

Foucault, M. (1978). "About the Concept of the 'Dangerous Individual' in 19th-Century Legal Psychiatry". Baudot, A., Couchman, J. (trans.). *International Journal of Law and Psychiatry.* Vol. 1. pp. 1.

Foucault, M. (1984). In P. Rabinow (Ed.), *The Foucault Reader*. London: Penguin. pp. 32-50.

Foucault, M. (1988) "Social Security". Politics, Philosophy, Culture. London: Routledge.

Foucault, M. (1995) *Discipline and Punish: The Birth of the Prison.* Sheridan, A. (trans). Second Ed. New York: Vintage Books.

Foucault, M. (1997) *Society Must be Defended*: *Lectures at the College de France* 1975-1976.

Foucault, M. (2000) "Technologies of the Self". Cited in Rabinow, P. (ed.) *Ethics: Subjectivity and Truth, Essential Works of Foucault, 1954–1984, Vol. 1*. New York: The New Press. P. 409

Foucault, M. (2003). *Society Must be Defended: Lectures at the College de France 1975-1976*. New York: Picador

Foucault (2007). *Security, Territory and Population: Lectures at the College de France 1977- 1978*. New York: Palgrave Macmillon.

Foucault, M. (2008) *The Birth of Biopolitics*, New York: Palgrave.

Frauley, J., Rigakos, G. (2011) "The Promise of Critical Realism: Toward a Post-Empiricist Criminology" in Doyle, A. Moore, D. (eds.) (2011) *Critical Criminology in Canada: New Voices, New Directions*. Vancouver. University of British Columbia Press. pp. 243-268.

Gandy, O. (2006) "Data-Mining, Surveillance and Discrimination in the Post-9/11 Environment". Chapter 15, In Haggerty, K., Ericson, R., V. (eds.) (2006) *The New Politics of Surveillance and Visibility*. Toronto: University of Toronto Press. pp. 363-384

Garfinkel, S. (2000) *Database Nation: The Death of Privacy in the 21st Century.* Beijing: O'Reilly. Cited in Aas, K., F. (2006) "'The Body Does Not Lie': Identity and Trust in Technoculture".Crime Media Culture. Vol. 2. pp. 143.

Garofolo, J. (1981) "The Fear of Crime: Causes and Consequences". *Journal of Criminal Law and Criminology.* Vol. 72(2). pp. 839-857.

Garland, D. (2001) *The Culture of Control: Crime and Social Order in Contemporary Society*. Chicago: University of Chicago Press.

Gates, K. (2010) "The Securitization of Financial Identity and the Expansion of the Consumer Credit Industry". *Journal of Communication Inquiry*. Vol. 34. pp. 417.

Gates, K. (2011) *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance*. New York and London: New York University Press.

Gesenhues, A. (2013) "Putting Facial Recognition Technology To Work For The Consumer: 5 Questions With Facedeals CEO". *Marketing Land.* Retrieved April 16th, 2014 via: http://marketingland.com/5-questions-with-facedeals-ceo-dave-mcmullen-59111

Gibson, M., Rafter, N., H. (trans., eds.) (2006) in Lombroso, C. (1876) *Criminal Man.* Durham and London: Duke University Press.

Giddens, A. (1985). *The Nation-State and Violence: Volume Two of a Contemporary Critique of Historical Materialism.* Berkley, Los Angeles: University of California Press.

Ginovsky, J. (2013) "Facial Recognition: The New Frontier". *ABA Banking Journal*. Retrieved April 11th, 2014 via: http://www.ababj.com/blogs-3/making-sense-of-it-all/item/4127-facial-recognition-the-new-frontier

Government Accountability Office (2011) "Defense Biometrics: DOD Can Better Conform to Standards and Share Biometric Information with Federal Agencies". Report to Congressional Requesters. GAO-11-276. Retrieved April 4th 2011 via: http://www.gao.gov/new.items/d11276.pdf

Greene, M. (2014, February) *Emerging Technologies and Innovative Biometric Research*. Presented at Biometrics for Government and National Security, Walter E. Washington Convention Center, Washington, District of Columbia.

Haggerty, K. (2006) "Tear Down the Walls" in Lyon, D. (2006) *Theorizing Surveillance.* Cited in Bauman, Z., Lyon, D. (2013) *Liquid Surveillance.* Cambridge: Polity Press.

Haggerty, K., Ericson, R., V. (eds.) (2006) *The New Politics of Surveillance and Visibility*. Toronto: University of Toronto Press.

Hall, S. (1995) "Introduction: Who Needs Identity?". In Hall, S., Du Gay, P. (eds.) (1995) *Questions of Cultural Identity*, London: Sage Publications.

Hall, J., L. (2012) "Facial Recognition & Privacy: An EU-US Perspective". *Center for Democracy and Technology*. Retrieved April 16th, 2014 via: https://www.cdt.org/files/pdfs/CDT_facial_recog.pdf

Haraway, D. (1998) *Modest_Witness@Second_Millenium.FemaleMan©_Meets_ OncoMouse.* New York: Routledge.

Haunss, S. (Forthcoming) "Mummery". To be published in Fahlenbrach, K., Klimke, M., Scharloth, J. (eds.) (Spring 2014) *Protest Cultures: A Companion. Vol 1: Elements of Protest.* New York : Berghahn Books.

Hawkesworth, M., E. (2006) *Feminist Inquiry: From Political Conviction to Methodological Innovation*. Rutgers University Press.

Hennessy, R. (2000) *Profit and Pleasure: Sexual Identities in Late Capitalism.* New York: Taylor & Francis Group.

Henry, A. (2013) "The Perpetual Object of Regulation: Privacy as Pacification". *Socialist Studies.* Vol. 9 (2). pp. 94-110.

Hodai, B. (2013, May) "Dissent or Terror: How the Nation's Counter Terrorism Apparatus, in Partnership with Corporate America, Turned on Occupy Wall Street". *Center for Media and Democracy*. DBA Press.

Hunt, A. (2004) "Getting Marx and Foucault into Bed Together!". *Journal of Law and Society.* Vol. 31 (4). pp. 592-609.

Ingersoll Rand (2014) "Case Study: Retail Sector: McDonald's is Lovin' the HandPunch". *Ingersoll Rand Security Technologies.* Retrieved April 16th 2014 via: http://security.ingersollrand.com/Downloads/Literature/Documents/McDonalds-LR%20copy.pdf

Introna, L., D., Wood, D. (2004) "Picturing Algorithmic Surveillance: The Politics of Facial Recognition Systems". *Surveillance and Society*. Vol. 2 (2/3). pp. 177-198.

Introna, L., Nissenbaum, H. (2010) "Facial Recognition Technology A Survey of Policy and Implementation Issues". *The Department of Organisation, Work and Technology.*

Jameson, W., C. (2005) *Billy the Kid: Beyond the Grave*. Taylor Trade Publishing.

Johnson, M., H. (2011) "Face Perception: A Developmental Perspective". Chapter 1 in Calder, A., Rhodes, G., Johnson, M., Haxby, J. (eds.) (2011) *Oxford Handbook of Face Perception*. Oxford, New York: Oxford University Press.

Jones, B., C., Little, A., C., Burt, D., M., Perrett, D., I. (2004). "When facial attractiveness is only skin deep". *Perception*. Vol. 33. pp. 569-576.

Jones, D. (2014, February) *Biometric Perspectives from the Intelligence Community*. Presented at Biometrics for Government and National Security, Walter E. Washington Convention Center, Washington, District of Columbia.

Journalistic Inc. (2014) "Beating the Buddy Punch". *QSR magazine*. Retrieved April 16th, 2014 via: http://www2.qsrmagazine.com/articles/tools/100/biometric_verification-1.phtml

Keen, S. (1986) *Faces of the Enemy: Reflections of the Hostile Imagination*. San Francisco: Harper and Row.

King, R. (2012) "Biometric Research Note: Asia to Lead Growth in Biometric Banking Applications". *Biometric Update.com.* Retrieved April 11th, 2014 via: http://www.biometricupdate.com/201212/asia-to-lead-growth-in-biometric-banking-applications

Klein, N. (2002) "Farewell to 'The End of History: Organization and Vision in Anti-Corporate Movements". *The Socialist Register.* pp. 1-14.

Klontz, J., C., Jain, A., K. (2013) "A Study on Unconstrained Facial Recognition Using the Boston Marathon Bombing Suspects". *Technical Report.* Michigan State University. MSU-CSE-13-4.

Kravets, D. (2014) "Federal Court Guts Net Neutrality Rules". *Wired.* Retrieved April 16th, 2014 via: http://www.wired.com/2014/01/court-kills-net-neutrality/

Kulka, R., A., Kessler, J., B. (1978) "Is Justice Really Blind?: The Influence of Litigant Physical Attractiveness on Juridical Judgment". *Journal of Applied Social Psychology*. Vol. 8(4). pp. 366–381.

Latour, B. (1993) *We Have Never Been Modern*. Porter, C. (trans). Cambridge, Massachusetts: Harvard University Press.

Lessig, L. (1999) *Code and Other Laws of Cyberspace.* Basic Books: New York.

Lianos, M., Douglas, M. (2000) "Dangerization and the End of Deviance". *British Journal of Criminology*. Vol. 40. pp. 261-278.

Lianos, M. (2003) "Social Control After Foucault". Surveillance and Society. Vol. 1(3). pp. 412.

Lianos, M. (2010) "Periopticon: Control Beyond Freedom and Coercion and Two Possible Advancements in the Social Sciences". *Surveillance and Democracy*. Routledge: Cavendish.

Lianos, M. (2012) The New Social Control: The Institutional Web, Normativity, and the Social Bond. Nice, R. (trans.). Ottawa: Red Quill Books.

Lombroso, C. (1876) *Criminal Man*. Gibson, M., Rafter, N., H. (trans., eds.) (2006). Durham and London: Duke University Press.

Lukács, G. (1971) *History and Class-Consciousness: Studies in Marxist Dialectics*. Merlin.

Lyon, D. (2001) *Surveillance Society: Monitoring Everyday Life.* Maidenhead: Open University Press.

Lyon, D. (2003) "Surveillance as Social Sorting: Computer Codes and Mobile Bodies" in Lyon, D. (ed.) *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*. pp. 13-30. London: Routledge.

Lyon, D. (2007) "Surveillance, Power, and Everyday Life" in Mansell, R., Avgerou, C., A., Quah, D., & Silverstone, R. (eds.) (2007) *The Oxford Hand Book of Information and Communication Technologies*. Oxford and New York : Oxford University Press. pp. 449-472.

Lyon, D. (2010) "Liquid Surveillance: The Contribution of Zygmunt Bauman to Surveillance Studies". International Political Sociology. Vol. 4. pp. 325-338.

Lyon, S. (2014, February) *Biometric Identity Services at DHS: Past, Present, and Future*. Presented at Biometrics for Government and National Security, Walter E. Washington Convention Center, Washington, District of Columbia.

Maudsley, H. (1868) "Illustrations of a Variety of Insanity". *Journal of Medical Science.* Vol. 14. pp. 149-162.

McCall, G., P., Rotenburg, M., Brody D. (2013) "Complaint for Injunctive Relief". Electronic Privacy Information Cenre V. Federal Bureau of Investigation. Retrieved April 4th, 2011 via: http://epic.org/foia/fbi/ngi/Complaint.pdf

Mears, J. (2014, February) *Possible Roles of Biometrics and Identity Technologies in Immigration Reform*. Presented at Biometrics for Government and National Security, Walter E. Washington Convention Center, Washington, District of Columbia.

Mockenstrum, L. (2002) "Testing Technology: From the Lab to the Field With Facial Recognition". *Corrections Today*. Vol. 64(3).

Mongia, R., V. (1999) "Race, Nationality, Mobility: A History of the Passport". *Public Culture.* Vol 11(3). pp. 527-555.

Negishi, K. (2013) "From Surveillant Text to Surveilling Device: The Face in Urban Transit Spaces". *Surveillance & Society.* Vol. 11(3). pp. 324-333

Neocleous, M. (2003) *Imagining the State.* Maidenhead, Philadelphia: Open University Press.

Neocleous, M. (2005) *The Monstrous and the Dead: Burke, Marx, Fascism.* Cromwell Press: Trowbridge, Wiltshire.

Neocleous, M. (2008) *Critique of Security*. McGill: Queen's University Pres.

Neocleous, M. (2013) "Resisting Resilience". *Radical Philosophy*. Vol. 178. pp. 1-7.

Neocleous, M., Rigakos, G. (eds.) (2011) *Anti-Security*. Ottawa, Ontario: Red Quill Books.

Newman, K. (1988) *Nightmare Movies: A Critical Guide to Contemporary Horror Films*. New York: Harmony Books.

Neyland, D. (2009) "Who's Who?: The Biometric Future and the Politics of Identity". European Journal of Criminology. Vol. 6: 135.

OPC Research Reports (2013) "Automated Facial Recognition in the Public and Private Sectors". *OPC Reports: Insights on Privacy.* Research Group, LSPR.

Paglen, T. (2011) "Contribution to Project: The Anxiety of Images". *Aperture 204*. pp. 67-68.

Pawson, R. (1989) *A Measure for Measures: A Manifesto for Empirical Sociology.* New York: Routledge.

Penton-Voak, I., Perrett, D., I. (2001) "Male Facial Attractiveness: Perceived Personality and Shifting Female Preference for Male Traits Across the Menstrual Cycle". *Advances in the Study of Behaviour.* Vol. 30. Academic Press. pp. 219-259.

Pieterse, J., N. (1992) *White on Black: Images of Africa and Blacks in Western Pop Culture*. New Haven: Yale University Press.

Pinedo, I. (1996) "Recreational Terror: Postmodern Elements of the Contemporary Horror Film". *Journal of Film and Video*. Vol. 48(1/2). pp. 17-31.

Press Association (2013) "Tesco's Plan to Tailor Adverts via Facial Recognition Stokes Privacy Fears". *The Guardian*. Retrieved April 11th, 2014 via: http://www.theguardian.com/business/2013/nov/03/privacy-tesco-scan-customers-faces

Rafter, N. (2008) "Criminology's Darkest Hour: Biocriminology in Nazi Germany". *Australian & New Zealand Journal of Criminology*. Vol. 41. pp. 287.

Raheja, M., H. (2011) *Reservation Reelism: Redfacing, Visual Sovereignty, and Representations of Native Americans in Film*. University of Nebraska Press.

Ratha, N. (2014, February) *Large-Scale Biometrics Search.* Presented at Biometrics for Government and National Security, Walter E. Washington Convention Center, Washington, District of Columbia.

Rigakos G., S. (2008) *Nightclub: Bouncers, Risk, and the Spectacle of Consumption.* Montreal: McGill-Queen's University Press.

Rigakos G., S. (2013) "Anti-Security Q & A: Interview of George S. Rigakos". Manolov, M., V. (interviewer). *The Annual Review of Interdisciplinary Justice Research*. pp. 9-25.

Rimke, H., Hunt, A. (2002) "From Sinners to Degenerates: The Medicalization of Morality in the 19th Century. History of the Human Sciences. Vol. 15 (1): 59.

Rimke, H. (2003). "Constituting Transgressive Interiorities: Nineteenth-Century Psychiatric Readings of Morally Mad Bodies" in A. Arturo (ed.) *Violence and the Body: Race, Gender and the State*. Indiana: Indiana University Press. pp. 403-28.

Rimke, H. (2010) "Remembering the Sociological Imagination: Transdisciplinarity, the Genealogical Method, and Epistemological Politics", *The International Journal of Interdisciplinary Social Sciences,* Vol. 5 (1). pp. 239.

Rimke (2011) "Security: Resistance" chapter 7 in Neocleous, M., Rigakos, G. (eds.) (2011) *Anti-Security*. Ottawa, Ontario: Red Quill Books. pp. 191-216.

Rissacher (2014, February) *Center for Identification Technology Research (CITeR)*. Presented atBiometrics for Government and National Security, Walter E. Washington Convention Center, Washington, District of Columbia.

Rose, N. (1999) *Powers of Freedom: Reframing Political Thought.* New York: Cambridge University Press.

Rush, B. (1839) *An Inquiry into the Influence of Physical Causes Upon the Moral Faculty.* Philadelphia: Barrington and Haswell.

Ryall, J. (2010) "Japanese Vending Machine Tells You What You Should Drink". *The Telegraph.* Retreieved April 11th, 2014 via: http://www.telegraph.co.uk /news/worldnews/asia/japan/8136743/Japanese-vending-machine-tells-you-what-you-should-drink.html

Sanburn, J. (2014) "Seattle Police to Use Facial Recognition Software". *TIME*. Retrieved April 11th, 2014 via: http://time.com/25605/seattle-police-to-use-facial-recognition-software/

Seri, G. (2011) "All the People Necessary Will Die to Achieve Security". In Neocleous, M., Rigakos, G. (eds.) (2011) *Anti-Security*. Red Quill Books: Ottawa, Ontario. pp. 243-264.

Shantz, J. (2011) *Active Anarchy: Political Practice in Contemporary Movements*. Lexington Books.

Sikka, T. (2006) "The New Imperialism: Using Critical Discourse Analysis and Articulation Theory to Study George W. Bush's Freedom Doctrine". *Global Change, Peace & Security.* Vol. 18 (2). pp. 101.

Sinclair, J., Coultard, M. (1975) *Towards an Analysis of Discourse*. Oxford: Oxford University Press.

Sixflags.com (2014) "Introducing a New Way to Enjoy Your Season Pass". *Six Flags*. Retrieved April 11th, 2014 via: https://web1.sixflags.com/national/footernav/biometrics.aspx

Smith, D. (1990) *The Conceptual Practices of Power: A Feminist Sociology of Knowledge*. Toronto: University of Toronto Press

Spisak, B., R., Homan, A., C., Grabo, A., Vugt, M., V. (2011) "Facing the Situation: Testing a Biosocial Contingency Model of Leadership in Intergroup Relations Using Masculine and Feminine Faces". *The Leadership Quarterly.* Elsevier. doi: 10.1016.

Star Wire Services (2011) Obituary: Osama bin Laden was the Face of Terrorism". *The Star.com World.* Retrieved April 14th, 2014 via: http://www.thestar.com/news/world/2011/05/02/obituary_osama_bin_laden_was_the_face_of_terrorism.html

Steel, E. (2011) "How a New Police Tool for Face Recognition Works". *Wall Street Journal.* Retrieved April 11th 2014 via: http://blogs.wsj.com/digits/2011/07/13/how-a-new-police-tool-for-face-recognition-works/

Stenman, J. (2013) "Embracing Big Brother: How Facial Recognition Could Help Fight Crime". *CNN.* Retrieved April 11th, 2014 via: http://www.cnn.com/2013/11/25/tech/embracing-big-brother-facial-recognition/

Strohm, C. (2013) "Facial Recognition on Facebook to IPhone Awaits U.S. Code". *Bloomberg News.* Retrieved April 16th, 2014 via: http://www.bloomberg.com/news/2013-12-16/facial-recognition-on-facebook-to-iphone-awaits-u-s-code.html

Stubbs, M. (1983) *Discourse Analysis.* Oxford: Blackwell. Cited in Teo, P. (2000) "Racism in the News: A Critical Discourse Analysis of News Reporting in Two

Takaki, R., T. (1979) *Iron Cages: Race and Culture in Nineteenth Century America.* New York: Knopf.

Teo, P. (2000) "Racism in the News: A Critical Discourse Analysis of News Reporting in Two Australian Newspapers". *Discourse Society*. Vol. 11. pp. 7.

Tinic, S. (2006) "(En)visioning the Televisual Audience: Revisiting Questions of Power in the Age of Interactive Television". Chapter 12, In Haggerty, K., Ericson, R., V. (eds.) (2006) *The New Politics of Surveillance and Visibility*. Toronto: University of Toronto Press. pp. 278-307.

Tudge, R. (2011) *The No-Nonsense Guide to Global Surveillance*. Ottawa, Ontario: New Internationalist Publications.

Tudor, A. (1989) *Monsters and Mad Scientists: A Cultural History of the Horror Movie*. Oxford: Basil Blackwell.

Turow, J. (2006) "Cracking the Consumer Code: Advertisers, Anxiety, and Surveillance in the Digital Age". Chapter 11, In Haggerty, K., Ericson, R., V. (eds.) (2006) *The New Politics of Surveillance and Visibility*. Toronto: University of Toronto Press. pp. 278-307.

Vemury, A. (2014, February) *Biometrics and Immigration Legislation*. Presented at Biometrics for Government and National Security, Walter E. Washington Convention Center, Washington, District of Columbia.

Vision-Box (2014) *VB Facelink: Advanced Biometric Identification System.* www.vision-box.com. (pamphlet).

Vrankulj, A. (2013) "NGI: A closer look at the FBI's billion-dollar biometric program". *Biometric Update.com.* Retrieved April 11th, 2014 via: http://www.biometricupdate.com/201311/ngi-a-closer-look-at-the-fbis-billion-dollar-biometric-program

Walby, K., Carrier, N. (2010) "The Rise of Biocriminology: Capturing Observable Bodily Economies of 'Criminal Man'". *Criminology and Criminal Justice.* Vol. 10(3). pp. 261-285.

Walters, W. (2012) *Governmentality: Critical Encounters*, Routledge.

Whitson, J., Haggerty, K., D. (2008) "Identity Theft and the Care of the Virtual Self". *Economy and Society*. Vol. 37(4). pp. 571-93

Willcocks, L. (2006) "Michel Foucault in the Social Study of ICTs: Critique and Reappraisal". *Social Science Computer Review*. Vol. 24(3). pp. 274-295

Williams, M. (2007) "Better Face-Recognition Software: Computers Outperform Humans at Recognizing Faces in Recent Tests". *MIT Technology Review.* Retrieved April 16th, 2014 via: http://www.technologyreview.com/news/407976/better-face-recognition-software/

Willis, D. (2000) *Reflections in Black: A History of Black Photographers 1840 to the Present*. 1st ed. New York: W.W. Norton & Company.

Winston (2013) "Facial Recognition, Once a Battlefield Tool, Lands in San Diego County". *Center for Investigative Reporting.* Retrieved April 11th, 2014 via: http://cironline.org/reports/facial-recognition-once-battlefield-tool-lands-san-diego-county-5502

Wodak, R., Meyer, M. (eds.) (2009) "Critical Discourse Analysis: History, Agenda, Theory and Methodlogy". Chapter 1. *Methods for Critical Discourse Analysis.* 2nd Ed. Sage Publications. pp. 1-33.

Zernike, K., Kaufman, M., T. (2011) "The Most Wanted Face of Terrorism". *The New York Times: World.* Retrieved April 14th, 2014 via: http://www.nytimes.com/2011/05/02/world/02osama-bin-laden-obituary.html?_r=0

Zinn, H. (2003) *A People's History of the United States.* New York: Harper Perennial/Modern Classics.

Zizek, S. (2010) "The Neighbor in Burka". *The Symptom.* 11:69