The Glut of Faciality: The Public/Private Face in Surveillance Culture

Kristina Fiedrich
CMNS 830
December 8th 2014

As a result of the rising culture of surveillance in the 21st Century, various sites of our bodies have become commoditized, embedding semiotic practices into seemingly objective forms of information gathering. This essay intends to explore the ways in which the face is being accessed by corporations as a personalized marketing tool, and policing/governing bodies as a means of surveilling and storing information. In this way the face has become a site of oscillation between publicness and privacy.

The term 'biometric' refers to the measurement of the physical body. Contemporary biometrics are rooted in earlier forms of surveillance and documentation techniques, including physiognomy, anthropometry and phrenology. Each of these historical methods are genealogically linked to the current modes of measuring, categorizing and 'datafying' the body. It is my aim to demonstrate how biometrics, specifically facial recognition software, motivates a new analysis of the face as an axis between what is public and private.

Starting with Michael Warner's historical analysis of public and private, this essay questions the position of the face when taken up as a set of information, biometric algorithms and codified analysis. I will argue that the amassing and distributing of identities by corporations and bodies of government denies the face as the place of private expression and turns it into an object of mass culture and commerce. With unprecedented access to personal information available through various platforms and technological mediation, this essay also takes up Mark Andrejevic's argument that the data-saturated world requires a reworking of the applications and politics of information sharing. In this way, I question the social and cultural acceptance and enthusiasm of technology as a universal remedy for behavior regulation and manipulation.

The Culture of Surveillance

The intention of this paper is to analyse the cultural phenomenon of biometric technologies. According to Jim McGuigan, cultural analysis is multidimensional, seeking "to make sense of the ontological complexity of cultural phenomenon […]. It is concerned with the circulation of culture and the interaction of production and consumption, including the materiality and significatory qualities of cultural forms." (1) Of particular concern are topics of public interest, issues of consequence to a democratic society, and questions that address wider, globally relevant concerns. While earlier methods of cultural analysis dealt with historical conditions, which McGuigan contributes to the assumption that the passage of time determined the importance of an event or phenomenon (3), current modes of cultural analysis typically study the present moment. This is attributed to the rise and saliency of mass popular culture.

Contemporary biometric technologies evoke social and ethical implications, and challenge issues of liberty, privacy and autonomy. While many biometric technologies involve what is referred to as "enrollment" – the voluntary submission of digitized representations of unique biological features for the purpose of future verification of identity – there are other non-voluntary systems implemented in modes of social control such as required personal identification documents. (Ajana 3; Alterman 140) Biometric techniques are rapidly becoming integrated into daily life, from digital fingerprinting used in border patrolling to closed-circuit television (CCTV) cameras for crime deterrence, and beyond, to high-tech "smart billboards" used for target marketing (Magnet 1). Surveillance casts a wide net, defined as the "purposeful, routine, systematic and focused attention paid to personal details, for the sake of control, entitlement, management, influence, or protection." (Wood qtd in Andrejevic et al. 189) The

symptom of being under surveillance engenders what Foucault refers to as "the conduct of conduct" in which we actively contribute to the policing of our own behaviour. Within the discourse of biometrics there are significant personal, political and social consequences, and the analysis of surveillance as a cultural phenomenon examines these concerns within the context of both public and private information. This essay will explore the specific biometrics of facial recognition as a lens through which to discuss the fluctuation of the face as publicly conspicuous and/or privately concealed. In this way, cultural analysis provides a contemporary perspective on 'public' and 'private' and how surveillance is impacting the socio-cultural space.

Public and Private

Historically, public and private have been understood as spatially distinct zones, such as the border between the home and place of business. What is considered public or private is embedded in instinctual behaviour and modes of speech. Social theorist Michael Warner refers to conventional public participation as a privilege that demands acceptable and conventional behaviour and the repression of private aspects of the self. (23) In this way the 'public' is a zone in which to perform a certain way, based on acceptable forms of behaviour, leaving the private within the walls of the home. These distinctions seem relatively easy to delineate and understand. However as Warner points out, public and private cannot always be located on a map: "Public and private sometimes compete, sometimes complement each other, and sometimes are merely parts of a larger series of classifications that includes, say, local, domestic, personal, political, economic or intimate." (28) So where does the body, and specifically the face, fit into the malleable concept of public and private?

The Western binary understanding of public/private has been long taken for granted. Privacy is considered a personal 'safe' space, concealed from the general public's view and free from the conventions of society and proper behaviour. Often privacy is considered an issue of controlling how and when we are represented to others. Anton Alterman describes this control as including the right to be safe from surveillance in the home, to choose with whom we are intimate, and the way we appear in public. When surveillance and documentation of our visible life is paired with the digitization of information, it is becoming essential to "retain the right to control the creation and use of representations which identify us, either through an image of parts of the body or through information indexed uniquely to an individual." (Alterman 144) As social theorist Btihaj Ajana points out technologies that capture the body are challenging the delineation between what is considered public and what can be deemed private. (8) In the case of the face, the conflict between public and private arises when considering notions of what is visible or concealed. The interest in maintaining a level of privacy, even when engaged in social/public activities, points to the body (and by extension the face) as integral to self-identity. The right to privacy also involves respect for our self and others as a means of maintaining what Ajana describes as "an inviolable personal 'zone'" (x). But by documenting, analyzing, sorting and storing information that would otherwise be considered in the realm of this 'personal zone,' what constitutes a violation of privacy is rapidly diminishing.

In March 2013 the Office of the Privacy Commissioner of Canada (OPC) reported on the developments, applications and potential risks of increasingly technologically efficient facial biometric software. The OPC had previously identified facial recognition "as having the potential to be the most highly invasive of the current popular biometric identifying technologies, since

the subject doesn't need to give consent or even participate knowingly." (1) While there are some benefits to facial recognition for the purpose of authentication of identity, the OPC and commentators on the technology warn that facial image data could result in the lack of all anonymity. What makes facial recognition software unique in techniques of surveillance is that images of the face can be taken from a distance without the individual's consent or knowledge. A 2011 study conducted at the Carnegie Mellon University demonstrated that facial recognition software could identify an individual based on facial images found on social media platforms. (2) This insinuates that any image shared on social media is fair game for use in surveillance and identification techniques and calls upon the public to become more aware of how and when their private images are being accessed or used without explicit permission. This has obvious implications for the individual's reasonable expectation for privacy, and engenders a public that is weary of always being under the watchful eye of surveillance technologies.

What is a face? As the site of identity and subjectivity, it assumes both an outward and inward reflection. Herein lies the duality of the face as both public and private. An open channel of communication to the public, it stands as an index for identification and public recognition; 'visibility' is a valuable commodity in the marketplace. The face is also personal, and the site of considerable sensory experience. It forms expressions of our most vulnerable and intimate moments and is a sign of personal identity. According to Kelly Gates, 'identity' is a dual concept that can both single an individual out via difference, or create associations through likeness. (15) The face is historically the most identifiable attribute and the human capacity to recognize faces is unmatched, save by the growing market of surveillance software. Images of the face have long been integral to self-identity formation, social documentation and identification management.

As Gates points out, “the ever present possibility of having personal photos appear on the Internet cannot help but change our sense of the boundaries around our private lives, and our sense of proprietorship and control over the full range of information that constitutes our identities.” (147) Increased surveillance and biometric technologies generate many representations of the face by which we can be identified, measured and sorted, resulting in what Alterman warns as “a loss of privacy, and a threat to the self-respect which privacy rights preserve.” (143) The spread of surveillance technologies and facial biometrics systems calls into question ‘identity’ itself, and “raises a need for exploring and understanding the intimate and intricate relationships between identity, body and information.” (Ajana 6)

Biometric technologies actively acquire, store and analyse biological information “whereby new forms of knowledge production are generated and […] the notion of ‘body as information’ is salient.” (Ajana 7) Facial biometrics and recognition technology treat the face as a static representation of identity. However, it is fluid and diverse in appearance, changing significantly through facial expression and in process of changing. The attempt to “bind identity to the body” (Gates 14) through a singular representation of the face breaks the body down into algorithms and dehumanized data sets. In this way, the body is being reconceptualised as publicly available human inventory and dramatically shifts the concept of privacy and personal information. (11) The quantity of information that is generated and made available in the digital age further exemplifies the need to question the changing status of public and private. The normalizing of surveillance and tracking systems, from tailored advertisements to facial recognition in social media photo-tagging, demonstrates social acceptance in our continuing loss

of privacy. Borrowing Mark Andrejevic's term of 'surveillance creep' (30), I will further explore the public/private dichotomy by addressing information sharing and the availability of data.

Database/Data-face

As previously mentioned, the goal of biometric technologies is to verify and authenticate identity. Taking measurements of the body, biometrics translates physiological information into algorithmic data. The defense of biometric data is that it avoids subjective interpretation, is proprietary (each facial recognition software develops its own algorithm) and cannot be 'stolen' or transferred from one individual to another. Biometrics therefore offer the convenience of assured identity and can be used to access personal accounts without having to rely on memory for passwords, PINs or cards. In this way, biometric technologies are promoted as providing evidence of truth, either of the individual's identity or specific intention.

Stemming from a long history of documenting and analysing the face as a visible representation of inner character and personality, contemporary facial recognition software continues to draw from scientific methods of information gathering to support its claim that the face, isolated in a photographic representation, can give away the truth. But if the face is an unfixed self-representation, fluid in its motions and characteristics, what is this fundamental truth? From a Foucauldian perspective, critical and cultural theorist Joseph Pugliese argues that, "truth emerges as a category that achieves its 'truth status,' so to speak, through the intertwining of regimes of power and knowledge that discursively determine and delimit the truth of a particular subject." (3) On one hand biometrics promises to bypass false or dishonest representation of identity, but is at the same decontextualizing the face itself. Embedded in

these record-making methods are racial and class stereotypes and predetermined judgements of character based on appearance. Anthropometrics, physiognomy, composite photography and eugenics are just some of the historical examples of face-based discrimination. Current technologies of facial recognition continue to participate in racial and social discrimination, abuse of power, and ways of seeing that shape the trajectory of public and private zones. In his discussion of the emergent surveillance society in the mid-aughts, David Lyon refers to surveillance as "social sorting," characterising the politics and practice of surveillance and the mediation of bodies and technology. Lyon writes, "surveillance today sorts people into categories, assigning worth or risk, in ways that have real effects on their life-chances. Deep discrimination occurs, thus making surveillance not merely a matter of personal privacy but of social justice." (Lyon qtd in Ajana, 8-9)

The accumulation of facial imaging data is rationalized for the purpose of social safety, personal security, tailored marketing, preventative measures and ease of use. Data storage is the new currency of communications and surveillance technologies, with increasing capacities to collect and process vast quantities of information. The creation of what Andrejevic and Gates refer to as "big data" provides "both unprecedented size of contemporary databases and the emerging techniques for making sense of them." (186) In this way, 'big data' doesn't just refer to the quantity of data available, but the uses to which it is put. These databases engender what Andrejevic considers to be an unreasonable expectation to predict (and ultimately prevent) unexpected, criminal and/or traumatic events. Further, the notion of intelligent, prophetic data, when combined with advanced computational power assumes that "the only limit on our predictive power is the ability to effectively organize all the available information." (20) The

result is an irrational faith in technology to not only govern our conduct, but prevent all future criminal acts. Data mining and information processing are "topic-agnostic," and Andrejevic highlights the limitations of predictive analytics, stating "[data sets] can be used in any context that calls for the extraction of useful patterns from large collections of data." (24) In this way, analytics can be tailored to provide a biased result, reinserting discriminatory, socio-cultural tropes and fears into scientific data. Andrejevic explains that, "[if] the imperative of data mining is to continue to gather more data about everything, its promise is to put this data to work, not necessarily to make sense of it. Indeed, the goal of both data mining and predictive analytics is to generate useful patterns that are far beyond the ability of the human mind to detect or even explain." (26) The patterns generated by the database are therefore subjective, taken out of context and made to provide information that mimics scientific data. (Andrejevic and Gates 186)

What is perhaps most unsettling is that data acquired today remains in play, with the potential to be accessed at an indeterminable later date. Data collected for a particular purpose can be reanalyzed to obtain a different pattern or outcome of information. (189) In their 2013 report, the OPC stressed that the storage of facial image information in databases challenges the right of personal privacy and requires legislation to moderate the need for restricted access. (7) The OPC's apprehension is centred on "the sharing of information with other agencies and governments, including law enforcement, with the risk of government tracking and surveillance without appropriate authorization, safeguards or oversight." And further, "federal government departments and agencies should implement and respect strict retention policies and dispose of the information once it is no longer required." (7) The unchecked amassing and retaining of

personal data, with or without consent or knowledge, is rapidly chipping away at what was earlier referred to in this essay as the 'inviolable personal zone.'

At present, government and national security agencies, telecommunications and marketing companies are the most commonly used examples associated with 'big data.' It would be wise, however, to consider the way in which the role of data analytics is growing to include other social practices, including finance, transportation, health care, employment, political participation and education. (189) There are many software applications that also promote the accumulation of data patterns to personalize experience, predicting musical selections, shopping preferences and media content. On the surface these customized, targeted marketing campaigns make the vast digitized network seem more personal. The predictive capacity of data analytics is uncanny in both its accuracy and relentlessness, and once again points to the so-called 'truth' of data. But the question remains whether we can avoid being coerced by habit-anticipated advertisements and be aware of how the private domain of our faces and bodies are measured, sorted and stored as depersonalized data.

The purpose of this essay was to explore the impact of surveillance on the conditions of public and private zones. Centering the discussion on the face, I have taken up facial recognition biometric technologies as the phenomenon against which to pitch these two spatialized concepts that delineate conduct and representation. From the outset, the challenge has been to conduct both the research and writing from an objective perspective, and to avoid a soap-box diatribe against the unlawful and unsanctioned surveillance of populations, the abuse of power and the decontextualized use of data. What has surfaced is the imperative for a reworking and

reorganization of the physical boundaries of the public and the private. As members of a socially driven society, the polarities of public and private have frequently been located and dislocated. With the invention of technologies of mass participation and surveillance, what I have argued is the face, as both visible and concealed identifier, demonstrates the oscillation and malleability of the terms of publicness and privacy. Though methods of social sorting and documentation have been threatening the individual's right to privacy for centuries, the advancements of technologically mediated methods of surveillance when paired with the steadily increasing demand and capacity for data storage is culminating in the elimination of anonymity. On one hand, the face is always external and visible to others. It is an index of identity and helps humans navigate the world through recognition, comparison and association. We can also subdue our thoughts and hide our true expressions, reserving the right to reveal our 'true' face in the safe space of privacy. The choice of how we are represented to others is inherent to the right to privacy. Surveillance and facial recognition technologies are essentially undermining the choice of representation. With access to our social media networks, images shared between friends and on websites are all become fair game in the monitoring, tracking, sorting, analysing and storing of our personal information, made data. Though some uses of our personal data is meant for the protection of identity and provides access to certain rights and freedoms (such as travel and banking), its accumulation can also be used out of context and for the purpose of pattern-detection, data analysis, and manipulation of scientifically findings. Transaction-generated data relating to patterns of consumption are classifying individuals based on presumptions of economic and political values. We are at a crucial moment in the development and implementation of biometric technologies, to be aware of their impact on our physical bodies

and faces, the translation of identity into data and the management of personal information by structures of control. While there are ways to trick biometric technologies, perhaps what is more important is to invest time and thought into whether the determination of privacy can be maintained. Warner's historical analysis of public and private terminology and its physical delineation points to the porousness of the concepts of inward/outward, visible/invisible representations of self. Surveillance and biometrics are closing in on the right to maintain obstructed from social, governmental, political or market control. Questioning the impact of biometrics and surveillance may not reverse what has already become the datafication and commodification of facial information, but may prevent what could result in a total loss of self-identification and private representation.

Bibliography

Ajana, Btihaj. “Introduction” and “Biometrics: The Remediation of Measure.” *Governing Through Biometrics: the Biopolitics of Identity.* Basingstoke: Palgrave Macmillan, 2013. 1-46. Print.

Alterman, Anton. "'A Piece of Yourself': Ethical Issues in Biometric Identification." *Ethics and Information Technology* 5 (2003): 139-150. Web. 11 Nov 2014.

Andrejevic, Mark. "Intelligence Glut: Policing, Security and Predictive Analytics.” *InfoGlut: How Too Much Information Is Changing the Way We Think and Know*. New York: Routledge, 2013. 19-41. Print.

Andrejevic, Mark and Kelly Gates. “Editorial. Big Data Surveillance: Introduction.” *Surveillance and Society.* 2 (2014): 185-196. Web. 1 Dec 2014.

Canada. Office of the Privacy Commissioner of Canada. Legal Services, Policy, Research and Technology Analysis Branch. *Automated Facial Recognition in the Public and Private Sectors.* Gatineau, QC: Research Group of the Office of the Privacy Commissioner of Canada. 2013. Web. 2 Nov 2014.

Gates, Kelly A. “Introduction: Experimenting with the Face.” *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance*. New York: New York University Press, 2011. 1-61. Print.

Gordon, Colin. "Governmental Rationality: An Introduction." *The Foucault Effect: Studies in Governmentality*. Ed. Graham Burchell, Colin Gordon, and Peter Miller. Chicago, IL: U of Chicago, 1991. 1-52. Print.

Magnet, Soshana A. *When Biometrics Fail: Gender, Race, and the Technology of Identity*. Durham, NC: Duke University Press, 2011. Print.

Warner, Michael. “Public and Private.” *Publics and Counterpublics.* Cambridge: Zone Books, 2002. 12-63. Print.