Article

Reimagining Resistance: Performing Transparency and Anonymity in Surveillance Art

Gary Kafer

University of Chicago, US.
gkafer@uchicago.edu

Abstract

In response to being detained and interrogated at an airport by the INS under false accusations, multimedia artist Hasan Elahi launched the project *Tracking Transience*, a website designed to constantly publicize his activity. Rather than uphold claims to privacy, Elahi aims to enact a resistive posture to contemporary techniques of digital surveillance by releasing his personal information. Paradoxically, he voluntarily forgoes his privacy in order to feel more secure. This form of resistance registers his project of self-surveillance as a performance of transparency. In this context, he turns the normative flow of power in digital surveillance into a new critical posture, one in which the artist is anonymous to surveillance systems. Through anonymity, the artist participates with digital surveillance in order to avoid it. By tracing the methodologies that generate data on Elahi's activity, this paper will speculate on how creative interventions can produce resistive strategies against surveillance systems by moving beyond the historical limits of privacy into the outer reaches of anonymity in our contemporary age of transparency.

*"Wile E. Coyote did finally catch the Roadrunner,
but then he held up a sign: 'What do I do now?'"¹*

Introduction

On June 19th 2002, the Immigration and Naturalization Service (INS) detained the Bangladeshi-American multimedia artist Hasan Elahi at a Detroit airport under the accusation of hoarding explosives in a Florida storage unit. After he was brought to the INS detention facility, he was questioned repeatedly on his whereabouts during the days surrounding the terrorist attacks of September 11, 2001. After six months of periodic interrogation at the INS facility, higher officials eventually dismissed all allegations against Elahi. However, he understood that his security was still under threat when he traveled by air, because INS officers at local airports would presumably continue to ethnically profile him, perhaps more now that he had a running file with the FBI.

Accordingly, Elahi decided to take preemptive action to avoid future altercations with federal authorities. Disclosing his entire history of banking records, phone records, airline travel, and even images of meals he had on airplanes, Elahi postulated that the more the FBI knew about him—the more he gave up his privacy—the more secure he would become. Taking this reasoning a step further, he ventured that if the public knew about his activity as well, then the value of his private information would diminish, and thus

¹ Epigraph previously published on Elahi's personal web page: <http://www.elahi.umd.edu/>.

have no capital gain for the FBI's surveillance. In this context, Elahi created software for his cell phone that tracks his whereabouts and uploads photographs to his website, *Tracking Transience: The Orwell Project* (<http://www.trackingtransience.net>), a massive online database of images and information designed to assist the FBI and the public with keeping track of his activity. While initially launched in 2002, the project has since been maintained as Elahi continues to update his website on a daily basis, sometimes even several times an hour, with new GPS coordinates and photographs.

The homepage of *Tracking Transience* displays two images. On the top is a photograph that Elahi has taken with his cell phone of his surroundings—a bedroom, an airport, a garage, a bathroom. Beneath it is a geo-tracking image taken from Google Maps and overlaid with an additional interface for identifying his coordinates. The bottom image borrows from surveillance strategies that employ geo-tracking, satellite triangulation, and digital cartography. The top image engages with the recent cultural shift into cell phone photography, online networking, and non-professional image-making practices, marked by a usually uninteresting perspective of a banal subject matter with such formal characteristics as blown out exposure, low digital quality, and blurred focus.

After about forty seconds, the website transitions to a new interface: a photomontage of images depicting a wide variety of objects and spaces. At this point, the user is able to click on and expand any image. Further clicking through these images will bring the user to different registers of the photomontage interface, each one centered upon a specific object or space. For example, clicking on an image of a bed will bring the user to a patchwork of beds in which Elahi has presumably slept. In most cases, the expanded image will have an overlay of white text detailing certain information corresponding to the photograph. This data ranges from the highly specific ("37.7433, -122.483, ~205.807 Saturday, 26 September 02:38:29 -0400 San Francisco, CA) to the incredibly vague ("August 17"), and in many cases to images with no text at all. Sometimes, there is no photograph, only text ("June 18 Hess 30500 East Brunswi [sic] NJ \$25.70"). Yet most frequently, the image is contextualized with only the corresponding day of the week and a date.

Despite the complete disclosure of Elahi's personal information in this format, *Tracking Transience* aims to enact a resistive posture to recent developments in digital surveillance. Rather than uphold claims to privacy, Elahi negotiates his security through the release of his personal information. Paradoxically, he voluntarily forgoes his privacy in order to feel more secure. This form of resistance then registers his project of self-surveillance as a performance of transparency. He turns the normative flow of power in digital surveillance into a new critical posture, wherein the artist becomes anonymous to surveillance systems and is able to maintain comfortable levels of security without typical recourse to privacy. And it is precisely this mode of anonymity that Elahi argues is able to produce a mode of resistance to surveillance, one in which the artist participates with digital surveillance in order to avoid it.

This project unfolds in three major sections. I first consider the current state of digital surveillance technologies and the treatment of data as the target of surveillance processing. Attention will then be given to the ways in which the normative discourse of the right to privacy has been challenged by contemporary surveillance and further altered in our current age of transparency. In the second section, I consider Elahi's project alongside prevailing debates concerning the possibility for aesthetic interventions to effect resistance to surveillance systems. The third section takes the title of Elahi's work—"tracking" and "transience"—as launching points to understand how his practice of self-surveillance simultaneously configures his resistance as a performance of transparency and anonymity. By tracing the methodologies that generate data on Elahi's activity, I will speculate on how creative interventions can reimagine resistive strategies against surveillance systems by moving beyond the historical limits of privacy into the outer reaches of anonymity in our contemporary age of transparency.

I. The Right to Privacy or the Desire for Transparency?

In contemporary surveillance tactics, human bodies are abstracted into a series of discrete flows of metadata through coded programs and algorithms, which are then reassembled to create profiles of those subjects of surveillance. These virtual profiles, or as Kevin Haggerty and Richard Ericson term them “data doubles,” are often not merely representations of people, but in fact constitute new individuals comprised of pure information, which are often regarded as more exact, legitimate, and authentic than their corresponding real bodies (Haggerty and Ericson 2000: 614). In this regime, surveillance systems increasingly track moving bodies rather than confining them to a fixed position. This trend in dataveillance, one of ‘mobile surveillance’ and ‘tracking in transit,’ gestures to a spatial and temporal shift in the operation of surveillance systems—confinement to mobility, past to future—in order to attain greater degrees of security for information, communications, and population management (Lyon 2007: 89). As such, contemporary surveillance opens up new issues for the right to privacy. For Haggerty and Ericson, privacy is now tempered by the “disappearance of disappearance,” such that privacy is increasingly difficult to achieve when bodies are continually made transparent to federal and corporate institutions as flows of data (Haggerty and Ericson 2000: 619).

Yet, this state of surveillance is not always imposed upon the subject—it is also increasingly being performed. When in 2004 open source software like Linux introduced a host of applications and service-oriented structures for the so-called Web 2.0, instruments for online “self-publication” inspired new forms of public communication (Zwerger and Medosch 2007: 18). It follows that, rather than privacy, Web 2.0 generates exposure. Over the past decade, discussions of privacy have become more attuned to the individual’s desire to share personal information in the public forum, most visibly through social media platforms. Of course, as is the case with nearly every technology in the digital age, engaging with such software necessitates a direct relationship with surveillance systems. The decision to log in to electronic telecommunication channels entails an implicit understanding of the costs and benefits of participating in the social field under the very conceivable threat of surveillance. Further, since surveillance constitutes a central organizing principle in the social field, efforts to achieve privacy are attended with abdicating certain social rights and benefits, such that privacy may very well impinge upon one’s participation within the social field. It follows that maintaining one’s privacy in the face of massive intelligence gathering systems, however noble and liberating it may be, negatively affects the context of embodying an active agency. Absolute privacy can only lead to ascetic isolation.

With the advent of digital communication technologies, what Lyon describes as the “surveillance society” (Lyon 1994: 3) —a mode of social practice based on and lived through surveillance—is now tempered with new issues regarding transparency. As Lyon points out, “knowledgeability” of surveillance by those under observation inspires “willing participation,” such that “surveillance works best with the cooperation of those who are subject to it” (Lyon 2007: 27). Accordingly, scholars have more recently attempted to theorize new types of societies marked by the increasing two-way flow of information in forms of public communication. In other words, the individual is transparent not only because of surveillance, but also because of voluntary and active self-exposure. David Brin calls this world of ever-present cameras and databases the “transparent society” (Brin 1998: 9) while Inke Arns refers to it as the “age of transparency” (Arns 2011: 256). Further, Bernard Harcourt places emphasis on active sharing, referring to this cultural moment as the “expository society” (Harcourt 2014: 11). Through whatever register one may wish to term contemporary experiences with surveillance, it is apparent that our desire to participate often overwhelms any feelings of insecurity or invasion of privacy. As Ina Zwerger and Armin Medosch contend: “We inhabit i-society: whether at iGoogle or iTunes, the desire to show what you’ve got is stronger than the fear of being monitored” (Zwerger and Medosch 2007: 18).

This type of subjectivity redirects the anxieties expressed about one’s data double into the precise desire for using the procedures of dataveillance to potentiate moments of affective, and possibly political,

engagements within the social field. In performing transparency, sharing one's personal life, seeking information, and connecting with others, one coheres a network of engagement based on the operations and possibilities of surveillance technologies that were once thought to pose a threat to those very forms of experience. From the rise of social networking sites like Facebook, Instagram, and LinkedIn to the proliferation of online dating services like Tinder and Grindr, transparency and exhibition assert a certain cultural cachet within the social field. For Harcourt, exposure as voluntary, active, and self-aware registers a change from Deleuze's "society of control," such that "we are not being surveilled today, so much as we are exposing or exhibiting ourselves knowingly and willingly, with all our love, lust, and passion" (Harcourt 2014: 11).

If surveillance is unavoidable and privacy seemingly unattainable, then in this context the real emphasis must be placed on transparency, both in term of surveilling organizations and the 'private' individual. On the one hand, federal and corporate institutions must be held accountable for using personal data to unethically impact individuals or certain populations. On the other hand, a greater understanding must be allotted to the ways in which sharing personal information on telecommunication channels, which today has become the dominant way to communicate, has formed new modes of subjectivity. Consequently, a new question emerges: as transparency increasingly becomes the dominant performative mode of participation in the social field, how can one resist surveillance and what does it look like? And further, in the case of Elahi's artistic intervention, how are aesthetics and politics reconfigured in transparency as a means of resisting surveillance?

II. Surveillance Art: Critique and Resistance

As a practicing artist, Elahi has exhibited *Tracking Transience* in a number of galleries and festivals, among them Kulturbahnhof (Kassel, Germany 2005), the Venice Biennale (Italy 2007), Sundance New Frontier (Utah 2008), Manifattura Tabacchi (Turin, Italy 2012), and Made in NY Media Center (Brooklyn, New York 2014). In these exhibitions, Elahi has continually recontextualized certain media from the website into independent pieces, such as *Altitude v3* (2007), a c-print of airline meals, and *Transit* (2011), a c-print of transportation spaces. It might be argued then that the political potential for Elahi's project is belied by its varying aesthetic reconfigurations in these works.

Yet on the other hand, *Tracking Transience* responds to an actual experience with political consequences: Elahi's detainment by government officials. Here, his work opens up space for effecting real change—physical, social, affective—to his experiences living under surveillance. In what follows, I will argue that the critical practice of surveillance art can be put into dialogue with the tactics of political resistance when attuned to the processes of dataveillance as an aesthetic intervention.

While in many ways Elahi's project can be considered as a relevant or even necessary tool to maintain a sense of personal security in response to his detainment by the INS, *Tracking Transience* in fact can be considered alongside a broader historical and aesthetic trajectory of surveillance art. Much more than merely depicting or representing surveillance as a topical issue, surveillance art formulates critical responses to the processes and technologies of monitoring, recording, and storing information on human activity. In this sense, surveillance artists need not exclusively use surveillance technologies or processes in their art making practice. Rather, they aim to mobilize a critical discourse on the rise and proliferation of surveillance in contemporary society by engaging with the politics and power relations configured by surveillance systems. Such practices may not always directly implicate certain bodies as targets of surveillance for the purposes of social critique, but rather construct networks of information exchange through which knowledge about bodies and human activity forms the basis of social relations represented and experienced in the work.

However, if one were to identify a broad development or trend among works in the context of surveillance, one would be compelled to acknowledge the overwhelming attention given to the visual register, wherein surveillance is most often crystallized by certain exchanges of power in the contemporary image economy. For Andrea Brighenti, surveillance art “can be interpreted as an attempt to deal with issues of social visibility and invisibility” invariably founded upon contemporary visual regimes and forms of recognition (2010: 138). Here, surveillance—whether structured through CCTV technology, telephotography, or spatial experiences—primarily rests upon the ability to see the surveilled subject, thus privileging the human body as the signifier of activity and identity.² Aesthetic critiques in this register emphasize re-constructing personal identities by gaining control of the production and circulation of bodies in this image economy. Manu Luksch’s *Faceless* (2007) and Jill Magid’s *Evidence Locker* (2004) are two such works that exemplify this approach, wherein both artists intercept CCTV footage of their bodies to construct alternative narratives and dispel feelings of insecurity.

Yet, if the technologies and systems of contemporary digital surveillance center primarily on information processing in order to maintain control over one’s data double, then the emphasis on the visual register in much of surveillance art seems to level a critique without engaging with the operations and agendas of current information gathering technologies. As argued by Katherine and David Barnard-Wills, whereas the majority of surveillance art operates within the visual register, dataveillance is concerned with the capture and collection of data. In this sense, much of surveillance art functions within the parameters of post-structuralist criticisms operative in art historical discourse, wherein identity as a performative and fluid condition can be located under the visual capture and collection of images of the human form. It is important to note in no way does this suggest that works engaging with dataveillance do not exist, but rather that aesthetic understandings of surveillance art tend to favor those works that can be situated within art historical discourses of vision, the image, and the human body.³

Such a focus on surveillance art sets into relief contentions with the ways in which contemporary forms of dataveillance structure and process identity. In post-structuralist discourses, individuals are able to assume or reject certain character and personality traits, particularly online where users of social networking platforms can produce and make visible any form of identity. However, following David Lyon’s definition of surveillance as “social sorting” (Lyon 2003), digital surveillance increasingly operates by extracting data on human activity and forcing it into specific categories and binary positions. Identity then is not something that individuals can control, but rather it is also assigned and administered across the social field by digital surveillance systems. Further, identity may not always be located on the human body; it may also emerge in virtual networks and circulate digital spaces.

Artists that engage with dataveillance thus posit a critique of surveillance not through the experiences of space or bodies, images and vision, or imaging technologies associated with the military-industrial

² Of course, the auditory register can also function as a means of surveillance, as made evident in such techniques as eavesdropping, wiretapping, and bugging. The point being, however, is that surveillance artworks by and large assume surveillance as a means of sensory uptake on information corresponding to certain activities related to the human body. While visual surveillance techniques dominant such art practices, auditory surveillance as well can be considered within this same paradigm, wherein surveillance locates upon the body one’s identity and subjectivity.

³ In justifying this claim, Katherine and David Barnard-Wills examine the 2001-2 exhibition *CTRL [SPACE]: Rhetorics of Surveillance from Bentham to Big Brother*, curated by Thomas Levine, Ursula Frohne, and Peter Weibel, a show which marked one of the first systematic overviews of surveillance art. They argue that while this exhibition claimed to interrogate the range of surveillance technologies, processes, and aesthetics from the architectural space of the Panopticon to the contemporary control over data, the exhibition overwhelmingly privileges work centered on the video camera, physical space, and the identity of the body. In the years following, this agenda did not change all that much; Tate Modern’s 2010 exhibition *Exposed: Voyeurism, Surveillance, and the Camera* managed to include only four works out of 185 that dealt primarily with dataveillance (Barnard-Wills 2012: 207).

complex, but rather through the tools and techniques operative within digital databases and information processing systems. According to Katherine and David Barnard-Wills, works that engage with dataveillance can be divided between two genres. On the one hand, there are works that deal with institutional and governmental intelligence gathering systems. On the other hand, there are also projects that engage with the surveillance of qualitative data generated by online technologies in conjunction with presumed forms of identity production. In both cases, these works leverage a critique on surveillance through a particular understanding of dataveillance and the ways in which identity can be created and limited through online platforms and information processing systems. Resistance in this sense does not aim to visualize certain identities or keep them hidden. Rather, resistance in the vein of dataveillance aims to manipulate protological measures in order to challenge the legitimacy of the data double and its relationship to its corresponding subject.

However, negotiating the boundary between critique and resistance is neither direct nor simple. It is not the case that criticism necessarily leads to resistance or that resistance is necessarily an element of critical practices. Surveillance art occupies a precarious position in this debate since surveillance work tends to engage with real technological systems with the potential for tangible and material consequences. In fact, resistance is central to the concerns of Surveillance Studies, which as a body of knowledge has attempted to schematize a range of possible practices of counter-surveillance. Gary Marx, for instance, offers twelve different types of neutralization techniques to surveillance practices, while further theorizing four counter-neutralization moves that may dispel resistive measures. While such a categorical argument risks leveraging political potency with a taxonomic interpretation, Marx brings to bear an important aspect of surveillance—that it is always attentive and responsive to resistive practices. He contends:

Neutralization is a dynamic adversarial social dance involving strategic moves and counter-moves [...] Those in the surveillance business respond to neutralization efforts with their own innovations which are then responded to in a re-occurring pattern. Whether for agents or subject, innovations may offer only temporary solutions. (Marx 2009: 299)

Resistance is thus part and parcel of surveillance strategies. And if this is the case, then the particular media involved in dataveillance as well contain within themselves the potential for resistance, and not just critique through aesthetic intervention. As Alexander Galloway argues: “If the network itself is political from the start, then any artistic practice within that network must engage politics or feign interest” (Galloway 2004: 214). Such practices then strategize resistive potentials through the very systems of control that negotiate their critique as a creative intervention. For Carolyn Guertin, resistance is enacted once the protocol of digital networks—or as Deleuze refers to it, the code (1992: 5)—is put into effect, thus opening up the potential of using that system for resistance:

But protocol works both ways. It can also become a means of using the system to enact resistance. Capture is a protocol and means of control within capitalist culture whether it is done technologically, visually, statistically, or physically. But capture, as an immovable force, always had its opposite built in. As soon as capture is enacted, leakage is inevitable. (Guertin 2012: 95)

Resistance then emerges from the very system of dataveillance, such that the rhetoric of digital surveillance technologies and processes can be utilized for political ends.

Following Jacques Rancière’s understanding of artistic practice as simultaneously aesthetic and political, it can thus be argued that for a work like *Tracking Transience*, which engages with surveillance through the protological network of web-based media, resistance is always already constituted in its aesthetic system. Concerning geopolitical approaches in contemporary art practice, Alan Ingram argues such work is “not just as a form of resistance, refusal or critique but [...] an index of and contributor to political and

spatial transformation” (2011: 218). Ingram does not quite parse clear distinctions between what makes a given work aesthetic rather than political, or in another register, what makes a work critical rather than resistive. Rather, he asserts that while it cannot be assumed that such creative interventions generate critical or radical results, they can produce the potential to represent ways in which discourses shaping social and political life might be reproduced, changed, or disrupted. The same logic can be applied to the field of surveillance art, wherein the emphasis is placed on the potential for artistic practices to mobilize other kinds of action in response to living under surveillance, rather than fully encompass the entire possible range of critical invention or political resistance.⁴

Importantly, artwork that performs transparency differs from the types of resistances practiced in work that attempts to hide the body or obstruct identity recognition software. For Torin Monahan, the latter prescribes to the discourse of the “right to hide,” which for him is a “weak variation of ‘the right to privacy,’” both of which “accept the legitimacy of state demands for legible populations and offer symbolic compromises to assert degrees of freedom within those constraints” (2015: 172), thus failing to challenge the violent demands of the surveillance state. Rather, through abandoning privacy and instead performing transparency, individuals may attempt to ascertain a degree of control over personal information, accessing one’s data double in order to complicate its circulation among information processing systems. These practices respond to dataveillance by intercepting information flows in order to formulate new relationships, narratives, and identities. In this context, performing transparency then allows one to sustain the type of security that one would normatively associate with the right to privacy.

III. Unpacking “Tracking Transience”

a. “Tracking”: Transparency in Dataveillance

For Inke Arns, there are two distinct methods of counter-surveillance when performing transparency: transparency *of* surveillance or transparency *through* surveillance. In the first case, one can make the structures of surveillance visible through direct intervention, such as the New York Civil Liberties Union *NYC Surveillance Camera Project* (<http://www.mediaeater.com/cameras>), which attempts to map every single public or private camera in Manhattan that records people in public space. In the second case, one can accept surveillance in order to become “invisible through maximum visibility,” or rather over-identifying with the surveillant regime, which renders one completely transparent (Arns 2011: 262-263).

Elahi’s project manages this second tactic of resistance, aestheticizing such systems with his technique of self-surveillance, and thus opening up space for security. In a *New York Times* Op-Ed published in 2011, Elahi remarks:

My activities may be more symbolic than not, but if 300 million people started sending private information to federal agents, the government would need to hire as many as another 300 million people, possibly more, to keep up with the information and we’d have to redesign our entire intelligence system [...] What I’m doing is no longer just an art project; creating our own archives has become so commonplace that we’re all—or at least

⁴ Raul Gshrey (2010:162) remarks that creative works can, depending on their contexts, move more or less towards art or political activism. In response to surveillance, artworks have the potential to raise awareness of the insidious effects of surveillance apparatuses, as well as make visible process of surveillance that demarcate and shape social spaces and experiences. Yet, unlike political activism towards surveillance, artworks do not need to elucidate answers, since they can be understood and experienced in many ways. Yet, this characteristic of the creative process should not relieve artists from having a social responsibility. Rather, they should take responsibility for the potential effect that their artwork can inspire within discourses running through the social field.

hundreds of millions of us—doing it all the time. Whether we know it or not. (Elahi 2011)⁵

By performing transparency, Elahi conceives of a radical potential in his project to disrupt the normative flow of power in surveillance. Here, he renders the commodity of surveillance—data—accessible to everyone, thus stripping that information of its value within the market of intelligence agencies. As he states in Marxist overtones in a 2008 interview on *The Colbert Report*, the logic of his performance responds to federal surveillance tactics by manipulating what he characterizes as “market forces” (Elahi 2008). Since intelligence agencies operate in an industry where their greatest commodity is information, the value of this data is directly correlated to its exclusive access for specific corporations, classes, individuals, and governments. In digital surveillance practices, various forms of exchanges between individuals and organizations are monitored and processed, thus producing a surplus of data. In order to refine services and target certain markets, corporations trace behaviors and generate interest profiles on their consumer base using this data surplus, which in turn results in a profit for those organizations. The more that corporations can predict networks of telecommunications activity, the more they can preemptively demarcate data flows to benefit capital investments. This is most evident in features like Google’s suggested search engine or Amazon’s recommended products page, algorithms that anticipate and control certain desires before the consumer takes action.

In contrast, Elahi’s practice of self-surveillance paradoxically generates a new surplus value of information at the same time that it produces its own conditions of surveillance. The artist thus negotiates a twist on the capitalist logic of federal surveillance, such that he is doing the work of data mining systems while simultaneously creating the very space in his project for those processes to exist. Consequently, he negates the profit that can be gained from constructing his corresponding data double through managing the production of his own personal information and having control on how that information might circulate other discourses of power.

Yet, while Elahi may speak of data, it is perhaps immediately apparent that Elahi’s performance of transparency locates that data in photographs that he uploads from his cell phone to construct his online archive of images. Arguably, this type of aesthetic practice operates along the visual register of surveillance, but fails to engage with the specific media and networks of information exchange particular to dataveillance.

Such a critical practice of transparency and self-surveillance aligns with Ai Weiwei’s project *WeiweiCam* (2012). Conceived in response to his detainment by Chinese officials at a Beijing airport and the following instalment of at least fifteen CCTV cameras observing his house, Weiwei decided to put himself under further surveillance to symbolically increase the aims of transparency negotiated by the Chinese government. The project consisted of four webcams that Weiwei mounted throughout his house, which sent a live 24-hour feed to the website <http://weiweicam.com>. Although Chinese officials shut down the project after 46 hours, *WeiweiCam* received more than five million views from the public worldwide. This project, which manifested as live CCTV footage on the website, engaged with surveillance by translating its visual rhetoric through the methodologies of self-surveillance and transparency. It should be noted that whether such a critical intervention with the Chinese authorities amounted to a mode of resistance is

⁵ It is important to note that, like privacy, transparency is coded as a privilege that only specific bodies and identities can perform. Elahi, who since the launch of his project in 2002 has become a reasonably successful contemporary artist and tenure-track professor, maintains a certain level of economic and cultural capital that allows him to enjoy transparency. Yet without the ability to generate data and harness this for personal use, self-exposure could portend dangerous consequences. Perhaps obliquely, Elahi’s project gestures to the uneven and hierarchical distribution of resources to perform transparency across the social field, or as Brighenti observes, “the emergent stratification of motilities and the dramatically curtailed freedom of movement migrants and minorities enjoy” (2010: 144).

perhaps difficult to determine, since Weiwei was still susceptible to the power dynamic assumed within his detainment and further complications with the government.

While *Tracking Transience* does indeed manifest surveillance as a visual rhetoric through its massive archive of photographs, Elahi in fact engages more closely with dataveillance despite his reliance on images and graphic interfaces. Rather than using self-surveillance like Weiwei to make the body transparent through visual evidence, Elahi downplays the importance of the image in his project, and emphasizes the way in which his project emerges through the means of data capture operative in dataveillance systems. These images—which normally index specific information on time, place, and behavior in surveillance systems—are simultaneously foregrounded as valuable because of the hyperactive gesture of being posted to the website, yet more importantly dismissed as easily consumable and virtually useless due to the website’s impenetrable interface. The image becomes a data point, rather than evidence.

Here, *Tracking Transience* manipulates the medium of protocol in order to produce its online archive. Despite the persistent emphasis on images, Elahi subordinates the importance of the photograph in order to prioritize the construction of his massive database as the primary project of his self-surveillance practice. In this case, the archive is not so much important for any real project of self-surveillance as it is for making space for an over-abundance of images which ostensibly represent certain types of information about the artist. The database then operates on the basis of form, rather than content. It is not so much imperative to depict what Elahi is doing at a given moment, but rather that some type of media is uploaded in the first place. The corresponding data double that emerges from his archive is not a complete account of his activity, but rather a hollow outline of his virtual identity, waiting to be filled with information that Elahi continually makes opaque under the guise of transparency.

It’s important to note that Elahi’s appropriation of the aesthetics of dataveillance is less an end product deployed for surveillance purposes than a procedure, or perhaps, in the words of John McGrath, a “performative” that can be enacted as a mode of resistance. For McGrath, contemporary surveillance constitutes a “surveillance space,” one that is spatially productive of certain performative effects that negotiate our subjectivities, as well as affective and ideological structures. This surveillance space is less a representational space in which surveillance operates, but rather it describes the ways in which the experience of surveillance is “lived and felt in spatial terms” (McGrath 2004: 134)—that is to say, the frames of presence and absence that circumscribe our bodies under surveillance. McGrath notes that a spatial analysis is also possible for dataveillance, which despite its resistance to both representation and conceptualization in visual terms, is still very much lived. Just as Elahi intentionally constructs an empty data double through his archival practice, McGrath notes that consciously living in the space of dataveillance allows for one to produce performative effects with resistive potentials:

When we accept or uptake this spatialization of data surveillance, that is to say when we knowingly situate our experience of data surveillance in relation to the uncrossable border and its production of doubles, the impasse of terrified good citizenship [...] potentially transforms into a very different spatial relationship. In this performative space of data surveillance—this particular space in which we cannot appear, in which we are (mis)represented by our own doubles, we may enact performances. Sending the consciously constructed bodies of credit, medical, immigration selves into the data zone, we may act parts on the stage of data surveillance—parts which, far from being etiolated in their effects, have real and dangerous consequences. (2004: 163)

As a result, Elahi’s performative tactics in the space of dataveillance qualifies the visual rhetoric of surveillance as ineffective for his project of transparency. Much like Debord’s concept of *détournement*, Elahi deterritorializes the rhetoric of dataveillance—code, protocol, data capture—by using its own

technology against itself, to produce self-surveillance without a subject. *Tracking Transience* simultaneously moves into a discourse of surveillance through its practice of voluntary self-exposure, but disrupts the legitimate exercise of information processing and storage practices in dataveillance through transparency. The project thus marks a resistance to surveillance at the same time that it allows for such surveillance practices to operate.

b. “*Transience*”: *Becoming Anonymous*

As previously argued, by aligning his project with the sort of activity observed on social media and other digital communications technologies, Elahi postures his project of resistance on the performance of transparency. However, Elahi’s attempt at resistance remains quite complicated. Despite the measures he employs in his project, Elahi is neither constantly nor permanently visible, since it is impossible to argue that he is completely transparent all the times or that he is disclosing every and all types of information to federal authorities. If this was the case, then Elahi perhaps would not be able to effect political resistance. Rather, he would be sacrificing his agency.

Yet, at the same time, it cannot be denied that *Tracking Transience* offers Elahi moments of escape from federal surveillance; the website’s interface presents complications in attempting to delineate a specific narrative of his current activity. Because Elahi’s GPS coordinates and cell phone photography are only periodically updated, these intermittent updates allow for slippages in the complete disclosure of his activities, such that he could, for example, easily make trips to a storage unit in Florida if he had the chance. In many ways, intermittent uploads in Elahi’s self-surveillance mimic social media, wherein status updates and tweets construct a narrative of self-created identity from discrete pieces of information. On the other hand, Elahi’s self-surveillance also emulates the type of information processing conducted by dataveillance systems, wherein only quantifiable activities and behaviors are recorded and stored for constructing one’s data double. At the intersection of these two registers of self-surveillance, Elahi’s project displaces the agenda of surveillance by simultaneously making room for the observation of federal authorities by continually updating his location and activities, but also obscuring his total transparency by disclosing only certain media at certain time periods under the guise of dataveillance techniques.

As *Tracking Transience* makes evident, the goal of resistance is not to fall outside of surveillance through privacy or to abolish surveillance altogether, but rather to share enough information in order to become invisible among others in public—physical, virtual, or otherwise. In another register, this type of engagement with surveillance can be regarded as anonymity, a condition of belonging without having any outstanding or unusual features. When anonymous, one participates in the social field, but is not recognized as an important subject for observation. Anonymity at once acknowledges surveillance as necessary for participation in the social field, but allows for moments of clearance by sharing information about oneself in order to be regarded as an autonomous agent. Anonymity understands that contemporary subjectivity is always already reproduced within the image of its own data double, such that one cannot exist without being a part of surveillance, yet proposes that challenging surveillance means working with it in order to be disregarded by information gathering and social sorting systems.

It is perhaps no coincidence that the catalyzing moment for Elahi’s project occurred in an airport, a type of space wherein anonymity under surveillance forms the prevailing mode of subjectivity. In airports, one must submit oneself to a highly orchestrated system of surveillance over passenger identities and the movement of bodies and objects. In such surveilled sites, one must present verification of one’s identity in order to pass customs and security checkpoints, and further allow for authorities to search and scan one’s body and luggage. Upon entering this space, one is cleared to become a traveler, one among many others who have likewise submitted themselves to this surveillance system. One has then become anonymous, abandoning one’s private identity in order to embody the subject position of the passenger.

In Elahi's case, the airport authorities flagged the artist because of his ethnic identity, thus preventing him from becoming anonymous. In this case, the ability to perform transparency and become anonymous is a privilege that can be granted or taken away from certain bodies and data doubles in varying types of surveillance spaces. In the airport, measures such as random selection and preferred passengers programs qualify anonymity by a certain status that one can achieve in systems of airport security. As Lyon observes:

Airports are perhaps the most stringently surveilled sites in terms of the means of movement and of identification. And they are also places par excellence for social sorting. [...] Although some treatments of airports romanticize them as points of departure for dream vacations and ultimate freedoms [...] in reality passage through the airport is highly uneven. (2007: 123)

Thus, just as the right to privacy is a privilege subject to exchange, and transparency a luxury that only certain types of bodies and identities are able to perform, anonymity as well is a commodity that can be distributed and denied according to the restrictions established by surveillance systems.

Lyon examines the degree of anonymity that one can achieve in airports as emergent from “‘non-places’ of consumption” (2007: 123). Here, he makes reference to Marc Augé’s theories on space and place. For Augé, the non-place is neither a negative quality of place nor the absence of place, but it is rather marked by a peculiar state of incompleteness as a proper place. Here, the non-place is one of movement and flux, a place of transit wherein stable identities and relations are not fixed or defined. In short, the non-place is one of transience. Examples of such non-spaces are bus stations and supermarkets: places that are not meant to be inhabited, but rather used for certain ends, such as transport, commerce, or leisure.

As is the case in airports, anonymity is an important quality of non-spaces. Whereas places produce social relations based on stable and fixed identities, non-places create what Augé terms “solitary contractuality” (1995: 94). This type of contract formed between the individual and the non-space describes a set of relations in which the individual achieves a certain autonomous anonymity in conjunction with the type of identity allowed within the non-place. For example, in the airport one must present identification in order to gain access to the transit space as a traveler. To quote Augé:

So the passenger accedes to his anonymity only when he has given proof of his identity; when he has countersigned (so to speak) the contract [...] Checks on the contract and the user’s identity, a priori or a posteriori, stamp the space of contemporary consumption with the sign of non-place: it can be entered only by the innocent. There will be no individualization (no right to anonymity) without identity checks. (1995: 101-102)

Paradoxically, identity must be verified in order for one to become an identity-less participant in the non-place. Anonymity in the non-place is not one of singularity, but of “solitude and similitude” (Augé 1995, 103). Since one can at once feel alone but also belonging to a larger network of social relations in non-places, anonymity can even be a site of security. As Augé observes, the traveler often feels most secure when participating in the anonymity of train platforms, convenience stores, and highways (1995: 106).

However, digital technologies of surveillance have changed non-places and the way that they produce varying identities and social relations. With the emergence of GPS (global positioning systems), mobile GIS (geographic informational systems) and other location-aware technologies, one’s position is always being tracked, monitored, and recorded. Even in non-places like airports, one is constantly under surveillance by geospatial interfaces, such that anonymity is increasingly qualified by a certain degree of spatial and temporal specificity. As Jordan Crandall remarks, digital technologies have produced the

“place-coded,” wherein real spaces, bodies, and objects are overlaid with information to produce a new virtual landscape (2006). Here, spaces are translated into an overexposed cartography, a map of transparency in which one’s identity is recognizable only as a data double. The type of anonymity in the non-place that Augé describes is then tempered by the existence of a quantifiable identity that is continually tracing one’s activity. One can become the anonymous traveler in the airport, but digital technologies will always perform that anonymity as transparent.

The question then is how to negotiate the desire for anonymity with one’s performance of transparency in order to effect resistance and achieve security? Just as the name of his project makes clear, Elahi’s goal is to foreground the complex relationship between transparency in the place-coded (i.e. “tracking”) with anonymity in the non-place (i.e. “transience”). On the one hand, Elahi’s project is performed in non-places, such as airports, bathrooms, hotel rooms, and highways. By representing these spaces on his website, he mobilizes the potential to achieve security in solitary contractuality. On the other hand, the constant status updates through his self-surveillance practice produces its own data double, thus doing the work of surveillance systems in order to reorient those non-places as place-coded.

The contention between these two discourses in *Tracking Transience* crystallizes in Elahi’s project through his treatment of the visual register of surveillance. While it was previously argued that Elahi downplays the importance of photography to his project of self-surveillance, it should be brought to attention that there is in fact a consistency and intentionality in the type of image that the artist produces. His photographs assume a constant vantage point correlating to what object or setting is being captured. For example, each image of a bed is shot from the same perspective. However, insofar as each bed, meal, road sign, or airport is imaged in the same exact way, it remains that the viewer is unable to position the subject within a specific locale, thus disturbing the specificity of the GPS data upon which the project of self-surveillance seemingly operates. The occlusion of any trace of Elahi’s body under this deliberate perspective hides his identity while substituting its existence with a labyrinthine patchwork of places, which indexes Elahi’s existence in as much as it serves as a proxy for it. By obscuring any visual evidence of his body in his data archive, Elahi manages to not only represent anonymity, but also produce it as the prevailing mode of subjectivity in his performance of transparency.

In this regard, *Tracking Transience* manifests a critical encounter with federal surveillance powers that functions upon its own impossibility of achieving either full anonymity or absolute transparency. Elahi’s resistance approaches anonymity to surveillance systems by giving the impression of transparency without really disclosing the relevant or necessary details of his activities. Here, he opens up a site for resistance by retracing his activities along an alternative surveillance aesthetic, one that deterritorializes the processing capacities of digital surveillance technologies in order to set into relief the limitations of those system’s abilities to actually achieve full transparency of their surveilled subjects. In this sense, it is not the case that Elahi wants to evade surveillance, but rather work within it as a participant in order to reimagine a new type of security in anonymity through the performance of transparency.

Conclusion

Resistance to digital surveillance programs in the age of transparency is one that actively participates in those very systems of data mining and information capture. It is one that seeks opportunities in standard operating procedures of surveillance to use the very same technologies in order to reclaim security even when that security is under constant threat—a radical practice that gestures to new ways of contesting surveillance while still relying on surveillance for one’s own benefit. In performing transparency, it may be possible to distill different forms of subjectivity in the contemporary information age, wherein disclosing personal information can expose new territory for living in surveillance as an anonymous subject, and perhaps more effectively maintain the humanist notions of freedom and security that are historically veiled within the “right to privacy.” As Elahi demonstrates, anonymity under transparency

may wield the hammer for demolishing the panopticon's looming silhouette from our contemporary skyline, revealing in the distance a horizon of data clouds, each one sparking with our desire to share more and more.

Acknowledgments

This author wishes to acknowledge the support of the Masters of Arts Program in the Humanities and the Department of Cinema and Media Studies at the University of Chicago. In particular, special thanks are extended to Dominique Bluher, who has provided gracious, patient, and challenging advising on this project.

References

- Arns, I. 2011. Transparent World: Minoritarian Tactics in the Age of Transparency. In *Interface Criticism: Esthetics Beyond Buttons*, eds by C. Andersen and S. Pold, 253-276. Aarhus: Aarhus University Press.
- Augé, M. 1995. *Non-Places: Introduction to an Anthropology of Supermodernity*, J. Howe (trans). London: Verso.
- Barnard-Wills, K. and D. Barnard-Wills. 2012. Invisible Surveillance in Visual Art. *Surveillance & Society* 10(3/4): 204-214.
- Brighenti, A.M. 2010. Artveillance: At the Crossroads of Art and Surveillance. *Surveillance & Society* 7(2): 137-148.
- Brin, D. 1998. *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?* Reading, MA: Addison-Wesley.
- Crandall, J. 2006. Precision + Guided + Seeing. *vector* 5 (July). Available at: http://www.virose.pt/vector/x_05/crandall.html.
- Deleuze, G. 1992. Postscript on the Societies of Control. *October* 59 (Winter): 3-7.
- Elahi, H. 2008. May 7, 2008: Hasan Elahi. *The Colbert Report*. Comedy Central. New York. Available at: <http://thecolbertreport.cc.com/videos/07p71k/hasan-elahi>.
- Elahi, H. 2011. You Want to Track Me? Here You Go, F.B.I. *New York Times*. Available at: <http://www.nytimes.com/2011/10/30/opinion/sunday/giving-the-fbi-what-it-wants.html>.
- Galloway, A. 2004. *Protocol: How Control Exists After Decentralization*. Cambridge, MA: MIT Press.
- Gshrey, R. 2010. Contemporary Closed-Circuits—Subversive Dialogues: Artistic Strategies Against Surveillance. *Surveillance & Society* 7(2): 144-164.
- Guertin, C. 2012. *Digital Prohibition: Piracy and Authorship in New Media Art*. London: Continuum.
- Haggerty, K. and R. V. Ericson. 2000. The Surveillant Assemblage. *British Journal of Sociology* 51(4): 605-622.
- Harcourt, B. 2014. Digital Security in the Expository Society: Spectacle, Surveillance, and Exhibition in the Neoliberal Age of Big Data. Columbia Public Law Research Paper No. 14-404. APSA 2014 Annual Meeting Paper.
- Ingram, A. R. 2011. Making geopolitics otherwise: artistic interventions in global political space. *The Geographical Journal* 177(3): 218-222.
- Lyon, D. 1994. *The Electronic Eye: The Rise of Surveillance Society*. Minneapolis: University of Minnesota Press.
- Lyon, D., ed. 2003. *Surveillance as Social Sorting: Privacy, risk, and digital discrimination*. London: Routledge.
- Lyon, D. 2007. *Surveillance Studies: An Overview*. Cambridge: Polity Press.
- Marx, G. 2009. A Tack in the Shoe and Taking off the Shoe: Neutralization and Counter-neutralization Dynamics. *Surveillance & Society* 6(3): 294-306.
- McGrath, J. 2004. *Loving Big Brother: Performance, Privacy and Surveillance Space*. London: Routledge.
- Monahan, T. 2015. The Right to Hide? Anti-Surveillance Camouflage and the Estheticization of Resistance. *Communication and Critical/Cultural Studies* 12(2): 159-178.
- Zwerger, I. and A. Medosch. 2007. "Goodbye Privacy! Hello Publicity?" In *Ars Electronica 2007: Goodbye Privacy*, eds. G. Stocker and C. Schöpf. M. Greenwald (trans). 16-20. Available at: <http://90.146.8.18>.