Iowa Research Online
The University of Iowa's Institutional Repository

Poroi
An Interdisciplinary Journal of Rhetorical Analysis and Invention
ISSN 2151-2957

Volume 16
Issue 1 *Big Data*

DOI: 10.13008/2151-2957.1287
Article 6

5-2021

Big Data Drive: The Rhetoric of Biometric Big Data

Valerie C. Ortega
California State University, Long Beach, valerie.ortega14@yahoo.com

Kevin Johnson
California State University, Long Beach, kevin.johnson@csulb.edu

This work is licensed under a Creative Commons Attribution-Noncommercial 4.0 License

Recommended Citation

Ortega, Valerie C.; and Johnson, Kevin. "Big Data Drive: The Rhetoric of Biometric Big Data." *Poroi* 16, Iss. 1 (2021): Article 6. https://doi.org/10.13008/2151-2957.1287

Hosted by Iowa Research Online

This Article is brought to you for free and open access by Iowa Research Online. It has been accepted for inclusion in Poroi by an authorized administrator of Iowa Research Online. For more information, please contact lib-ir@uiowa.edu.

Big Data Drive: The Rhetoric of Biometric Big Data

Acknowledgements

The authors would like to thank Amanda Axley and the Editorial Staff of the POROI journal for their extensive and generous comments and editing labor.

This article is available in Poroi: https://ir.uiowa.edu/poroi/vol16/iss1/6

Big Data Drive:

The Rhetoric of Biometric Big Data

Valerie Ortega
California State University
Long Beach, CA

Kevin A. Johnson
California State University
Long Beach, CA

Poroi 16,1 (May 2021)

Abstract: In this essay, we seek to develop the concept of big data drive. Influenced in part by Lacan's theory of drive, we study the drive toward biometric big data (BBD), which refers to the data collected by facial recognition, eye recognition, thumb prints, and other types of technology whose task is to identify a specific person through unique bio-characteristics. Big data drive refers to the energies that pulsate around big data as both a signifier and fetishized object to promise something more that may never be fulfilled.

Keywords: Big data, biometrics, drive, rhetorical envelopes, technology, rhetoric

Introduction

Despite the overwhelming distrust of big data, our information society perpetuates constant and copious data-collection, leading to a struggle as we embrace big data while simultaneously resisting it. In recent years, tensions regarding the particular meanings ascribed to big data have risen. Big data is the large quantity of data that is computed and analyzed to create patterns and generalizations about a population in what Roberto Simanowski (2016) refers to as the "data love phenomenon not only of a society of control but also of the consumer society" (p. xiii). Additionally, Jake Porway, founder and executive director of DataKind, stated that big data "presents tremendous opportunity for the social sector to gather and analyze information faster to address some of our world's most pressing challenges" (2014). As a form of rhetoric, big data functions as both a mechanism of control, and a mechanism of freedom. Therefore, we will analyze the psychic investments of engaging in the rhetoric of big data, both in terms of the dystopian fantasies constituted by control and surveillance, and the utopian

fantasies constituted by convenience and its promise to solve the world's problems.

Conversations surrounding big data have always been present, but recent events (e.g., iPhone X facial recognition technology, the Equifax data breach, and the Facebook and Cambridge Analytica scandal) have drawn attention to the various implications of the uses for big data. In a 2013 *Wall Street Journal* op-ed, Senator Dianne Feinstein indicated that big data in the call-records database is used for preventing terror attacks, declaring that "Working in combination, the call-records database and other NSA programs have aided efforts by U.S. intelligence agencies to disrupt terrorism in the U.S.". Furthermore, in 2017, Amazon CEO Jeff Bezos alluded in a letter to shareholders to the use of big data, writing that "At Amazon, we've been engaged in the practical application of machine learning. … Machine learning drives our algorithms for demand forecasting, product search ranking, product and deals recommendations" (qtd. in LaFrance, 2017). Feinstein and Bezos both reference big data as significant for systemic development and improvement. On the other hand, United States Federal Trade Commissioner Julie Brill, in a speech about privacy and security in the age of big data at the Cyber Security and Privacy Summit, stated that "As we add devices to our homes, classrooms, and clothes, much more sensitive data will be collected. User interfaces on devices will shrink or disappear" (2016). Brill goes on to say that the minimization of big data boundaries then "pose[s] difficult challenges for privacy, security, and fairness in our society." Therefore, while big data can indeed improve or aid in the development of societies, it also raises pressing concerns about privacy for the user and the ways we collect, analyze, and use the data. Simanowski accounts for the opposition of meanings about big data in his description of a phenomenon he calls data love, which paradoxically "thrives on precisely the same data that security and privacy claim to protect" (2016, p. xiii). In other words, data love grows on promises of safety and security while simultaneously deteriorating on the same promises it inevitably fails to keep.

Big data's contested ideological investments all highlight a worldwide drive toward big data. Accordingly, we seek to develop a better understanding of this phenomenon and apply drive theory to the drive toward biometric big data (BBD). BBD refers to the data collected by facial recognition, eye recognition, thumb prints, and other types of technology whose task is to identify a specific person

through unique bio characteristics (Techopedia, n.d.). Collectively, people are driven toward the reinforcement and pursuit of big data as a mass cultural phenomenon. To understand what *drives* individuals to the world of big data, we will use a psychoanalytic approach to explore drive in a Lacanian sense.

Our goal is to examine the particular fantasies at the center of the drive toward big data. In doing so, we will first unpack Lacan's drive theory and define big data drive. Next, we will utilize the concept of drive to analyze big data drive in the rhetoric of biometric big data.[1] We will conclude by expanding on the significance of our analysis of big data drive and biometric rhetoric as a tool in discerning the way big data functions as an iteration of the Symbolic and by exploring the distinct meanings ascribed to big data based on various fundamental fantasies.

The Theorization of Drive and Big Data

A psychoanalytic approach which interrogates humanity's subjective attachment to objects in the world offers a fascinating angle on the problem of big data. A Lacanian psychoanalysis of the issue begins with questions of the subject's attachment to big data; indeed, Lacan alludes to these kinds of human motivations in his formulation of drive theory, where he asserts that people are driven to particular signifiers because they are latent with particular promises of fulfillment that can never actually be satisfied. By its nature, the purpose of the Lacanian drive "is not some mythical goal of full satisfaction, but to return to its circular path, and the real source of enjoyment is the repetitive movement of this closed circuit" (Evans, 1996, p. 47).

Taken together, big data drive refers to the energies that pulsate around big data as both a signifier and fetishized object, to promise something more that may never be fulfilled. In this way, big data signifies certain promises for the subject, which direct the relationship to and fetishization of particular objects of desire. Therefore, big data functions tropologically by way of being the signifier that is the locus of directing particular fantasies, configuring multiple meanings about big data. The way in which big

[1] When we use the term "rhetoric of biometric big data," we refer to the way that big data are used as a language and/or rhetorical device to represent particular ways of meaning in terms of our relationship to and with big data.

data accomplishes various symbolic ways of meaning is how it functions tropologically—by acting as a trope for different fantasies. Big data drive then encloses the subject in a rhetorical envelope, and the drive hinges on the desire it dissatisfies. Big data drive requires fantasy to assert itself: without desire, there is no fantasy, and without fantasy, there is no drive. Therefore, to understand big data drive in its full complexity, we must first examine the way in which a drive comes to be.

In their work on the iPod as a fetishized gadget, Gunn and Hall (2008) explain that "The drive represents a culturally mediated state of lack" (p. 142). This state of lack "signifies a lack in the Other" where the Other refers to the Symbolic order in which language constitutes the subject (Evans, 1996, p. 7). Thus, the subject exists through the Symbolic, which is bound up by various linked signifiers—the signifying chain. Because the signifying chain can never be completed, as it "always lacks the signifier that could complete it," a state of lack is produced, and thus desire comes to be (Evans, 1996, p. 96). Big data then can never actually fulfill a person's desires because "the (un)conscious recognition of lack is always already a symbolic process" (Gunn & Hall, 2008, p. 7). In other words, big data as signifier produces different meanings to certain people, and because there is always a signifier missing in linkage to big data, there is room for something more, enabling the perpetual nature of desire. In this way, "the failure of unicity necessitates imagined unicity to purchase the coherence of a subject's 'reality'" (Lundberg, 2012, p. 2), hence the particular fantasies inferred in the discourse surrounding big data. Representative of this is the discourse of big data as a way to improve quality of life by providing "better insights for eradicating poverty" (Pokhriyal et al., 2015). However, this iteration of big data fails in its unicity of the subject in that it also simultaneously functions as a way of "trapping those who do not have a voice, instead of improving their lives" (Waddell, 2016). By examining the language surrounding big data, we can see a distinct phantasmic idea about what big data is or should be and how it fails in its unicity of the subject due to differing particular fantasies (after all, the Imaginary is a "social field of deceptions" (Gunn, 2003, p. 43)). Big data drive then positions the Imaginary as the fundamental defining quality of this drive.

These fantasies are designated through the Imaginary, where the identity of the subject is located "as a process of amalgamating more and more instances of replication and resemblance in order to

bolster up the fable of unicity" (Myers, 2004, p. 8). In other words, a subject constructs their own place in reality through the Imaginary by way of fantasies, conjuring up the unicity of the subject and then creating meaning through different forms of language-signifiers. Hence, big data operates by its tropological function, which Lundberg defines as "the relationship between the sign and the genesis of the subject … constitut[ing] the subject and its imagined modes of social relation" (2012, p. 8). Thus, big data functions tropologically as it acts as the signifier at the core of the relationship between other signifiers and the core of particular fantasies of different individuals with those signifiers.

We can see big data's tropological function at work in the discussion of big data for policing. For instance, New York City Police Commissioner William Bratton declared that predictive policing "is the wave of the future" (qtd. in Winston, 2015). His rhetoric demonstrates the utopic fantasy whereby police officers deal with criminals before they commit a crime (similar, to the way officers operate in the popular film Minority Report). However, in their work on stochastic governance, Sanders and Sheptycki (2017) argue that big data has become part of the means of production that are made possible by a panoptic sort that results in the discipline and categorization of those who are subject to the elite. Specifically, they argue that "what is new is that the 'means of production' now include the technologies that make 'Big Data' possible" (p. 5). Sanders and Sheptycki also draw from the work of Gandy as they explain that "these technologies underlie the 'panoptic sort'" (2017, p. 9). Gandy argues that the panoptic sort becomes significant as it is "configured by stochastic governance into cybernetic social triage which privileges elites while it disciplines and categorizes the rest" (Sanders & Sheptycki, 2017, p. 9). Taken together, then, big data may operate as a means of production that functions as a panoptic sort for the privileged elites while simultaneously classifying and punishing others. If big data is viewed as both a wave of the future for policing and also a discriminatory process, then big data drive works tropologically upon the Real in that the subject's fantasies manifest meaning into big data. Big data becomes the "site of a number of elements of failed unicity" (Lundberg, 2012, p. 9), and the way it is interpreted differently is its tropological function, which also unveils the existence of the Real.

However, the desire steering these fantasies is embedded with failure because the "illusion of unicity is a scandalous lie" (Lundberg, 2012, p. 9). The failed unicity of the subject then causes

the subject to reinvest in these fantasies, thus manifesting in themself a drive toward big data. In this way, it is the failed unicity of these fantasies that propels the subject back into the continuous cycle constituting big data drive. Drive then is when "humans are coerced into thinking and behaving in reference to energies that pulsate around certain objects" (Gunn & Hall, 2008, p. 9).

In regards to the Real interrupting the fantasies of big data, we can assess the rhetoric surrounding the failure of the 2016 presidential election polls, when Donald Trump beat Hillary Clinton despite all polls predicting a Clinton victory, thus illustrating the collapse of big data's meaning. Bill Schmarzo, chief technology officer of the Big Data Practice of EMC Global Services, stated that political polling uses "tons of big data" to "try to predict on a county by county basis who's going to show up" (qtd. in Woodie, 2016). In this sense, the big data fantasy concerns election predictions. Nevertheless, big data fails, and the moment of collapse when confronted with Clinton's loss—because of the Real—then manifests as fantasies of order. Michele Chambers, the CMO and EVP of Continuum Analytics, was implying this particular fantasy when she asserted that "The lesson learned is we have to improve the way we model for elections" and that "Adding facial recognition and doing linguistic analysis is really going to net them much more precise results" (qtd. in Woodie, 2016), subsequently exposing how the Imaginary reinvests in the big data fantasy in the wake of its encounter with the Real. These reinvestments then conceal the failed unicity—interruptions made by the Real—of the subject and the Other; these interruptions then "become the driving [force] that animate[s] human existence" (Lundberg, 2012, p. 10), thereby providing "a schema according to which certain objects can function as objects of desire" (Žižek, 1997a, p. 10).

Žižek (1997a) references this type of drive toward an object of desire when he expounds on commodity fetishism: "Commodity fetishism is thus a strange intermediate stage between fetishized social relations and transparent social relations: a stage in which social relations are no longer fetishized, yet fetishism is transposed on to '(social) relations between things'" (p. 100). In other words, commodity fetish is the way big data drive propels the subject in the direction of desired material objects (Evans, 1996, p. 10) that promise the fulfillment of a particular fantasy (e.g., iPhones) as individuals interpret the object as a parallel to a specific signifier and fantasy.

Žižek provides the example of a king whose status as king is only real in as much as the subjects treat him as one. Referring then to the Hegelian notion of reflective determination, Žižek states that the king is fetishized as he is "misperceived" in his "direct 'natural' property"—the point here is that fetishization occurs at the moment where the "natural" person (reduced to biology/physiology as not much distinctive with other people) takes on the symbolism of "king" and thus becomes "attached" to the fantasy of kingdom (Žižek, 1997a, p. 10). In relation to big data, we can see that the fantasies drive the subject toward a commodity fetish; thus, the relationship with this particular object of desire only works in as much as it "fits the subject's particular fantasy" (Žižek, 1997a, p. 11).

The process of fetishizing a king is homologous with the process of fetishizing big data. Expanding on the previous example of the failure of the 2016 election polls, we can see the fantasy surrounding the polls and the use of better "data-gathering techniques, such as facial and linguistic analytics" to make the polls—big data—better (Woodie, 2016). This fantasy would then lead to the commodity fetish of big data as, for example, facial recognition technology. On the other hand, the phantasmic view of the poll failure sees it as a problem not of big data but of the underperformance of humans, thus positioning "sharper reporting, a clearer read on the numbers and a more penetrating portrait of on-the-ground realities" as the only ways to collect better data (Timms, 2016). In this way, the object at the center of an individual's desire is based on their personal fantasy about big data, so while facial recognition technology may become the fetishized object for one individual, it may not for another. What allows big data to have currency in the first place is the way that different people are driven to it, which then directs various people and energies into big data, enabling all commodity manifestations that flow from it.

Gunn and Hall refer to the commodity fetish of big data drive as a gadget to represent a drive that promises fulfillment of desires. They describe the iPod as a rhetorically promising desire that can never be fulfilled, resulting in a continuous drive and persisting desire. They state that "one cannot separate the physical excitation of the drive from the fetishized", meaning that the iPod cannot be separated from the drive toward its fetishization and the experience of its use (2008, p. 142). In this respect, big data drive perpetuates desire of the commodity fetish because the subject is unable to separate the fetish character of big data from the experience of the

materiality. Big data acts on people through language denoting different fantasies and setting forth a drive to various experiences of its materiality. Language encapsulates the subject; because the subject is "an independent system, forming its own closed world" (Myers, 2004, p. 12), they enclose themselves in their own reality through language. In turn, by using language to signify different fantasies, the subject is wrapped into a rhetorical envelope in the world of big data.

The rhetorical envelope relates to big data drive by (falsely) fulfilling people's desire. Drawing from Gunn and Hall's concept of the "sonorous envelope" (2008, p. 12), the rhetorical envelope names more formal characteristics whereby we create bubbles that hinder encounters with each other or any unpleasant interaction. Gunn and Hall describe the sonorous envelope as the "representation of losing one's self in music," in which those engaged "regress to a blissfully anterior (i.e., pre-subjective, pre-linguistic, pre-Oedipal) state" (2008, p. 12). In relation to the rhetorical envelope, the same functions are created within the subject, but it names the confining of people from discomfort in various ways. For instance, in the context of big data, a rhetorical envelope might form when people talk about the Internet's filter bubble, a term coined by Eli Pariser in his analysis of Facebook's feed-filtering. Pariser noticed that many of his conservative friends' posts were missing from his Facebook feed, leading to his discovery that Facebook was tracking which links he clicked more frequently. Because he clicked more on his liberal friends' links, Facebook had filtered his conservative friends' posts out. He stated that "Facebook isn't the only place that's doing this kind of invisible, algorithmic editing of the Web. Google's doing it too," referring to Google's tailored search results, which returns different search results for different people (2011a). In other words, the web was becoming more personalized by using everyone's data to tailor the user experience to individual needs and desires. Specifically, Pariser states that "personalization filters serve up a kind of invisible autopropaganda" which increases our desire for ideas and objects that we are already familiar with but leaves us "oblivious to the dangers lurking in the dark territory of the unknown" (2011b, p. 15). The filter bubble then leaves less room for chance and more room for the familiar (Pariser, 2011b, p. 12).

The rhetorical envelope guides our understanding of what Pariser argues about the personalization of information made possible by big data. According to Simanowski, "Personalization algorithms

suppress chance and encounters with the Other and thus can be said to generate a kind of information specific xenophobia of which, for the most part, one is not even aware" (2016, p. 13). Big data creates patterns and generalizations, appearing to fulfill the subject's desire of "cognitive consistency" (Simanowski, 2016, p. 13), or as Pariser argues, it "creates the impression that our narrow self-interest is all that exists" (2011b, p. 108). This creates the desire for the fetishized object and encloses the subject in a rhetorical envelope, which safeguards the subject from encounters with the Real by negotiating any chance encounters. Deriving from what Gunn and Hall state about the iPod as being able to "seamlessly mix thousands of songs from one's personal library into a seemingly endless playlist" (2008, p. 143), the rhetorical envelope affords the subject an endless consistency. As in the case of the filter bubble, individuals are consistently ensured that information they like will be present on their timeline. The drive for big data, as in the case of the iPod, "can therefore pulsate endlessly, freed from the end of the record" (Gunn & Hall, 2008, p. 13).

Big data drive is bound in the fantasies about big data, with big data acting as the master signifier as these fantasies are "structured by the symbolic (or linguistic) order because no image or representation can be expressed absent its symbolization as a signifier" (Gunn, 2003, p. 13). The external material feature of big data is revealed as "people are reduced to instruments sacrificed as the pedestal for the specter of the future New Man," thus creating an "ideological monster" from big data drive (Žižek, 1997a, p. 13). This ideological monster is akin to positioning big data so it may function as Žižek's "maternal Thing that 'swallow's' the subject" (1998, p. 250). Because big data saturates all that the subject is, it may function in a manner Žižek describes as "a dystopian prospect of individuals regressing to presymbolic psychotic immersion," paradoxically "losing the symbolic distance" (1998, p. 13). This is the conflicting relation on which big data drive hinges.

In Simanowski's work concerning what he called the "cold civil war" within each citizen, he argues that citizens are caught in between the interest of technological progression and the discomfort of being watched and controlled by the same technology. The "cold civil war" is what "hinders all attempts at strengthening data protection" because what could weaken corporations' usage of data structures would also "rob the citizenry of many advantages that are a result of the centralization and interconnection of data" (Simanowski, 2016, p. 14). This indicates

the perpetual seduction and betrayal of big data that is necessarily the way that fantasy functions—the defense mechanism against radical nothingness of the subject and the fantasies in iterations of betrayal. The phantasmic rhetorical nature of big data drive as "the signifier which forbids the subject access to X"—meaning big data forbids access to certain things such as autonomy—then "gives rise to phantom" (Žižek, 1997a, p. 14). In this sense, big data drive is an iteration of the Symbolic. The conflicting interacting fantasies aid in our understanding of the relations to these technologies because "Lacan opens a path to think of the Symbolic as specifically tropological and, therefore, as a rhetorical phenomenon" (Lundberg, 2004, p. 14). In this way, big data drive is akin to Boyle's (2016) description of the impact of technology entering into "intense social relations with itself" (p. 273). Drawing on the work of Rickert's "ambient rhetoric," Boyle (2016) explains that such technological contexts function rhetorically "not in the sense that we have rhetorical deliberation or exchange" (Rickert, 2013, p. 32) but "in the sense that the values and decisions that emerge from and are built into the ensemble of interacting elements result from rhetoric, and, conversely, in rhetorical interaction" (Rickert, 2013, p. 32). Accordingly, the application of big data drive identifies the desires and the subsequent fantasies of the subject that interact with the fetishized object of big data.

Big Data Drive in the Rhetoric of Biometrics

The notion of big data was first presented by Michael Cox and David Ellsworth when they referred to the "problem of big data", stating that "when data sets do not fit in main memory (in core), or when they do not fit even on local disk, the most common solution is to acquire more resources" (1997, p. 235). The birth of the big data phenomenon is apparent in Google CEO Eric Schmidt's comment on the exponential explosion of data: "From the dawn of civilization to 2003, five exabytes of data were created. The same amount was created in the last two days" (qtd. in Carlson, 2010). Although biometric data dates back to 1902 and the first "systematic use of fingerprints in the U.S. by the New York Civil Service Commission" (*The history of fingerprints*, 2017) there has been a vast growth in its use in more recent years, with a projected "4.8 billion biometric devices by 2020" (Violino, 2015). The rapid growth of biometric big data has several implications for society.

In relation to security, Kelly A. Gates states that "the aftermath of 9/11 was a moment of articulation, where objects or events that

have no necessary connection come together and a new discourse formation is established: automated facial recognition as a homeland security technology" (2011, p. 100). This reached the mainstream when airports began the use of BBD as a means of security. Andy Bien, chief information officer of Airport Authority Hong Kong, explained that the use of facial recognition technology was "at the center of a triple-pronged strategy to enhance operational efficiency, deliver retail benefits, and optimize asset management" (*Airport Authority*, 2017). A BBD drive is evident here as a means of national security and is even suggested to benefit consumers.

As for the relation to consumerism, Simanowski (2016) references the 2011 Berlin conference Data Love, where it was declared that in today's data-driven economy the consumer is the focal point, challenging many to create new applications out of the ever-growing data stream. Because data now determines "who wins, what lasts and what will be sold", it is the "crucial driver to develop relevant products and services for the consumer" (Simanowski, 2016, p. xii). In the rhetoric of biometrics, this is apparent when individuals talk about Fingopay, a finger vein payment technology. Industry professionals must constantly adapt to the rapidly changing, data-based market; for example, Nick Dryden, chief executive of Fingopay's parent company Sthaler, said that "Today's millennial generation now expects a higher level of ease, security and efficiency from the way that we pay" (qtd. in Baron & Dorfer, 2015). Bryan Campbell, senior security researcher at Fujitsu UK&I, has stated that "There is no silver bullet for stopping identity fraud for good, but from contactless palm vein scanning to iris scanners; biometrics is essential for protecting both consumers and organizations in a data driven world" (qtd. in Nunns, 2017). These discussions regarding payment technology demonstrate that when it comes to the consumer, security drives the BBD.

Conversely, where there is a desire for better security, there is also a desire for privacy. Simanowski argues that "Smart things can only communicate to one another what they know about us, and if their service is based on intimate knowledge, then the breach of privacy happens for the sake of efficiency rather than control" (2016, p. 17). In this rhetoric we see a promise of improved consumer experience through the generalizations made by big data, within which the concern for privacy becomes naturally interwoven. This is made apparent as surveillance systems for law-enforcement grow rapidly in the name of security. The FBI's official Biometric Center of

Excellence (BCOE) page declares that "Improv[ing] national security by developing and deploying biometric technologies" is a "biometric priority" (n.d.). However, these systems become invasive when they are not controlled and become "profound threats to commonly accepted notions of privacy and security … the people behind the controls can actively track you throughout your daily life" (Scientific American, 2014). Within this perspective, individuals are driven to big data even as it means privacy theft and, in a way, theft of an individual's autonomy and/or identity.

Information is now used for both the needs of consumerism and better security, but with these needs BBD has created many anxieties regarding privacy concerns as biometric data capture an individual's most private features; this then explains the fantasies people manifest to deal with these inconsistencies regarding the attraction and repulsion of BBD. The tensions arising from the rhetoric of BBD is where the desire for big data comes from. That is, the imbalance within the psyche is "constitutive of human desire" (Žižek, 1997a, p. 17), which then steers the big data drive. Therefore, the rhetoric of BBD is a meaningful artifact to examine the big data drive. When analyzing the big data drive in the rhetoric of BBD, we establish that there are four main components to this rhetoric: (1) commodity fetish and big data; (2) capital accumulation; (3) security/privacy; and (4) rhetorical envelopes.

Commodity Fetish and Big Data

The commodity fetish is evident in the use of BBD as the technology that makes its use possible becomes the object of desire as they fulfill the fantasies attached to them. At the heart of the drive toward BBD are the fantasies of better protections and the benefits provided by such technologies, though there are also consequential fantasies of such technologies. Nevertheless, the fetishized commodity stays the same, as it is still the object at the locus of the fantasy. For example, the world's largest use of BBD, the Aadhaar identification system, has "recorded the biometric details of over 1 billion Indians" (Sethi & Bansal, 2017), situating the Aadhaar database as a "classic definition of a Big Data system" (King, 2015). The system uses a range of products designed by software company MapR to provide the security it promises, including a biometric reader, a host computer, biometric ID card, and servers (Sethi & Bansal, 2017). The co-founder and CEO of MapR, John Schroeder, believes that "the implementation of such a big data storage architecture … will allow India to have advantages in terms of

delivering healthcare, insurance and other social services"; in fact, "The entire technology architecture behind Aadhaar is based on principles of openness, linear scalability, strong security, and most importantly vendor neutrality" (King, 2015).

Particular fantasies are at play here (e.g., security and advantages in multiple social services), and the commodities delivering these promises become susceptible to individuals' desires. The desired object here is the biometric ID card provided to all identification system registrants. To receive the desired ID card, people must enroll in the program; with about "one million new enrollments every day", individuals can satisfy the fantasies they have prescribed upon the ID card such as being able to pay taxes, collect pensions, and obtain certain welfare benefits (Bengali, 2017).

The ID card, as an object of desire, doubles as both an entity of the identification system and as an embodiment of an ideal such as security and/or attainment of certain benefits. As desire only aims "to reproduce itself as desire" (Žižek, 1997a, p. 39), it inherently fails, hence the failure of the commodity fetish to fulfill the subject's fantasies, thereupon exposing the perils of big data drive. The promises made by the BBD system Aadhaar become complicated as the once voluntary system becomes mandatory in order to receive said promises. The commodity fetish remains as the biometric ID card by way of the tropological function of big data drive. The tropological function of the drive toward the biometric ID card is that it now signifies not only a voluntary force but a mandatory one as well, for without it, "it becomes difficult to open a bank account, get a new cellphone number or buy plane or train tickets" (Bengali, 2017). The driving fantasy for the citizen now becomes one of a desire for inclusion in a variety of services, whereas for the government the desire for inclusion is a way "that will transform governance" (Bengali, 2017). The differing fantasies associated with the biometric ID card then perpetuate the big data drive because at the core of these fantasies is the signifier of big data. The failure of the initial desire of the ID card as a means to fulfill promises supports the repetitive compulsion of the big data drive and the utility of the biometric technologies.

When it comes to predictive policing, cameras are the most obvious form of commodity fetish. The fantasies associated with the commodity fetish of the camera and predictive policing are of the technologies as a means of crime forecasting and/or security. With the growth of big data, police departments are using big data as a

means to "inform and deploy" (Jagadish, 2015). For example, Lawrence Byrne (qtd. in Neubauer, 2015) argued that the public benefits of data-gathering from phones, body cameras, and other technologies far outweigh concerns from some advocates about privacy and predictive policing. In other words, the fantasy alluded to in the use of these surveillance tools is the fantasy of public safety, which manifests as a desire for the material object—the camera—and ascribes the meaning of safety. Big data is used in predictive policing for the "mining of huge amounts of information and developing algorithms that will effectively mine that data in many ways the human brain cannot" (Winston, 2015), which is seen in the context of biometrics when discussing the use of facial recognition technology by police departments. Cameras (e.g., street surveillance cameras and police body cameras) become the desired object in satisfying the fantasy of public safety, made apparent in the use of "real time video feed facial recognition" and on any "cameras, drone footage, and body-worn cameras" (including those of police officers) (Garvie & Moy, 2019). The fantasies in relation to the use of BBD then produce a big data drive within affairs such as predictive policing. But because the essential part of the drive is the betrayal of the very desire conceived by the fantasy, the desire for public safety betrays the citizens' desire for protection of privacy. As Lever (2017) states, "Civil liberties activists who fear the technology could lead to secret 'profiling' and misuse of data" (Para. 4) demonstrate the anxieties surrounding the very betrayal of the desire on which big data drive depends.

Capital Accumulation and Biometric Big Data Drive

Biometric big data has been discussed in terms of enhancing customer experience (*Biometric system*, 2003) and analyzing productivity (Mezzofiore, 2017), both of which drive capital accumulation. Illustrative of this is the FindFace app, which was released by a Russian tech company for "emotion reading recognition"; the app can "track everyone on VKontakte, the Russian equivalent of Twitter, based on their profile" (Mezzofiore, 2017). The app is said to help not only law enforcement, as it can "search through a database of a billion faces in less than half a second … with 73% accuracy with a database of 1 million pictures", but is said to be of possible use in "dating, security, banking, retail, entertainment, and events" (Mezzofiore, 2017). When combined with big data, behavioral analytics suggest it could be used for

"customer behavior analysis" (Mezzofiore, 2017). CEO Mikhail Ivanov explained its purpose is "to track the level of service on your customers, to understand the behaviors of the guy you're going to hire based on his emotional reactions during a job interview, to grasp the emotions of a crowd during a concert, and their emotional temperature" in order to analyze the data and enhance productivity (qtd. in Mezzofiore, 2017). In the context of big data drive, the desire for customer assessment and better productivity for capital accumulation is the driving force to use BBD.

Paul Denimarck, Donald Bellis, Jr., and Clarke McAllister patented technology in 2003 that used big data to

> biometrically identify a customer of a retail or non-retail establishment to facilitate or enhance the customers shopping experience. The method includes obtaining a biometric profile representation of a biometric characteristic of a customer using a biometric sensor device; retrieving shopping history related information for the customer based on the biometric profile. (*Biometric system*, 2003).

Identified here is the use of biometric technology resulting from the desire for enhanced customer experience. In the patent, they outline advantages attributed to the technology, such as the ability to "reduce or eliminate the need for check-out employees … thereby reducing labor costs associated with retailer operation and/or labor time…" (*Biometric system*, 2003). The BBD technology also aids in making businesses less susceptible to labor shortages while still maintaining their services (*Biometric system*, 2003). The distinct fantasy behind the patented technology is driven by the desire to enhance the customer experience; thus, capital accumulation is made possible by BBD by reducing costs. It is unsurprising that big data directs the particular fantasies of businesses and consumers; businesses reflect the fantasy of cost reduction while consumers reflect fantasies of enhanced shopping experiences, substantiating the individual fantasies and desires that maintain the big data drive.

Security vs. Privacy and Biometric Big Data Drive

Psychologically, we know that stories that offer a sense of security are powerful. Edkins (2015), for example, observed that, "We are susceptible to narratives of insecurity and threat, and tempted by

promises of security" (pp. 108–9). The psychological description is significant because the very desire that drives the fantasy of better security comes into contact with the fantasies of individual autonomy and privacy, and all of which become apparent in the existence of big data drive. We see the most profound use of BBD technologies for security purposes in law enforcement agencies, so much so that a Biometric Center of Excellence was created by the FBI. The website for the BCOE states that it is "strengthening criminal investigations and enhancing national security, while ensuring compliance with privacy laws, policies, and regulations" (n.d.). While citizens want to be protected from possible terror threats, they do not want their privacy infringed upon. Research by the Georgetown Law Center on Privacy and Technology, however, states that "Police use of face recognition is inevitable" and that the technology already "affects over 117 million American adults" (Garvie *et al.*, 2016). The use of BBD technologies is also often unregulated, and "Across the country, state and local police departments are building their own face recognition systems, many of them more advanced than the FBI's" (Garvie *et al.*, 2016). This has left the public unaware of the implications this may have on their "privacy and civil liberties" (Garvie *et al.*, 2016).

Furthermore, research by the Human Rights Data Analysis Group (HRDAG) demonstrates "the mechanism by which the use of predictive software may amplify the biases that already pervade our criminal justice system" (Lum, 2016). In other words, HRDAG argues that the big data promise of security betrays one of the very things it asserts to protect: secure privacy protection. From that perspective, the big data drive is preserved as the drive is directed to the paranoia of crime that already lurks in the data. In his work on "pervasive citizenship," Boyle notes that "We see such advances toward data-driven governance take form in how many governments, corporations, and researchers laud 'big data' as a panacea for many of our civic problems, creating so called 'smart' and 'sentient' cities" (2016, p. 22). Essentially, Boyle argues that government is driven to big data through the fantasies of safe cites and solutions to problems. The commodity object that attempts to satisfy these fantasies is facial recognition technology. But this comes at the expense of the very rights the government sets out to protect, and thus the solution creates even more problems. Constant surveillance is ubiquitous; in his book *Surveillance Society: Monitoring Everyday Life*, David Lyon (2002) states that "in the UK cameras have become a common sight" (p. 62). More importantly, he contends that these cameras address the fear of

crime, though they do not stop the fear of crime, while at the same time feelings of safety do not increase. However, installing cameras has slightly decreased for many the "fear of being a victim" (Lyon, 2002, p. 63). The cameras are only a presentation created by the anxieties surrounding crime, thus the desire to stop crime manifests into a fantasy to cope with the anxiety.

The same could be said when put in the context of BBD. For example, the surveillance used by police forces to better predict criminal activity may not accurately perform its intended function but instead conceals the anxieties produced by the criminal activity while also causing anxieties over privacy concerns. This is a major concern amongst advocates against BBD as it "could turn existing surveillance systems into something categorically new—something more powerful and much more invasive" (Hendrix, 2013, p. 1). In a talk on the controversial Domain Awareness System, attorney Jennifer Lynch of the nonprofit group Electronic Frontier Foundation discusses the "network of 3,000 surveillance cameras in New York City" (Scientific American, 2014). She states that cops have the ability to review sections of video, but if the systems were equipped with facial-recognition technology, those analyzing the footage would be able to "actively track you throughout your daily life" (Scientific American, 2014). Drawing on the work of Foucault (1977), Simon (2005) discussed this state of constant surveillance in the contemporary era. Simon (2005) explained,

> The panoptic structure seems to speak to the sense of the helplessness individuals often feel in the face of overwhelming force of institutions (prisons, hospitals, schools, workplaces, families) to determine life within their confines … the sense that there is nowhere to run and nowhere to hide. (p. 3).

In view of the statement made by Jennifer Lynch, we can see how the constant surveillance made possible by BBD becomes a portrayal of the Panopticon itself. Therefore, this anxiety then constitutes big data drive. As Evans (1996) explains, Lacan relates anxiety to desire by arguing that "desire is a remedy for anxiety, something easier to bear than anxiety itself" (p. 24). The big data drive and its fantasies of protection and security finds a way to ease the subject of the panoptic possibilities.

Rhetorical Envelopes of Big Data Drive

The compulsive nature of big data drive repeatedly encloses the subject in a rhetorical envelope which is articulated in the rhetoric surrounding the use of BBD. Subsequently, it is apparent how the use of BBD for predictive policing serves to enclose individuals in a rhetorical envelope. Predictive policing is often suggested as a way "the police can anticipate a crime and be there to stop it before it happens and/or apprehend the culprits right away" (Jagadish, 2015); this anticipation of crime and prevention before it takes place is the very characterization of the rhetorical envelope.

In 2016, the Canadian border started testing the Automated Virtual Agent for Truth Assessment in Real Time (AVATAR) to "help agents screen for criminals and even potential terrorists" (MacDonald, 2016). The AVATAR would ask a series of questions and, by the use of biometric data, would detect if the individual was being deceptive and possibly "flag the passenger for further inspection" (MacDonald, 2016). The researchers stated that "The system can detect changes in the eyes, voice, gestures, and posture to determine potential risk. It can even tell when you're curling your toes" (MacDonald, 2016). They also stated the potential for the AVATAR to be used across many industries as a preventative method. It is within this promise of the prevention of a disturbing or unpleasant encounter, such as a terror attack, that the big data drive rhetorical envelope resides.

Furthermore, we can see a more recent iteration of this promise and the drive toward BBD in its use for immigration purposes. A provision in President Donald Trump's (2017) executive order on immigration mentions BBD as a tracking system for the potential prevention of terror attacks. The provision reads:

> Sec. 7. Expedited Completion of the Biometric Entry-Exit Tracking System. (a) The Secretary of Homeland Security shall expedite the completion and implementation of a biometric entry-exit tracking system for all travelers to the United States, as recommended by the National Commission on Terrorist Attacks Upon the United States. (Trump, 2017)

The provision alludes to the fantasy of protection for the nation, thereby positioning the object of desire as a tracking system that itself doubles as the fantasy of protection from terrorists. The entry-

exit system enables more accurate matches and prevents more errors than previous systems which used only biographic data. For example, the misspelling of the 2013 Boston marathon bomber's name, Tamerlan Tsarnaev, resulted in "the FBI missing a lead while investigating his terrorist ties" (Sternstein, 2014). Using BBD can help avoid these errors while simultaneously preventing encounters with threatening forces. The use of BBD negotiates these unpleasant encounters before they are experienced, thus hindering encounters with the Real (e.g., threatening criminal encounters). The rhetorical envelope created by the fantasy of protection from threats then allows the big data drive to pulsate endlessly. In this way, the rhetorical envelope of big data drive created by particular fantasies encloses the subject in the world of big data to prevent encounters with unfamiliar and menacing entities.

Conclusion

Using psychoanalysis, we have argued that the fantasies alluded to in big data rhetoric are explained through the theorization of big data drive, and we explored the particular fantasies and desires behind the drive. We specifically applied big data drive to the rhetoric of BBD and in turn characterized the drive in terms of its creation of the commodity fetish; the fantasies regarding capital accumulation, security, and privacy concerns that produce big data drive; and its enclosure of the subject in a rhetorical envelope. The fantasies perpetuating big data drive work together tropologically, allowing for the construction of big data's meaning while also making evident the subject's differing relations to big data, thus acting as the very thing that directs each subject's particular fantasies. When applied to the rhetoric of BBD, the paradox of BBD technologies as both a means of security or prevention and as a breach of privacy can be better understood through the theorization of big data drive. Additionally, as the use of big data technology rises, so too do the potential benefits and risks.

As such, the implications of the big data drive are twofold. The first is the theorization of big data drive as inherent to the way the technologies of the self operate when it comes to the subjective relationship to big data. Technologies of the self are those which permit the subject to start regulating the self. Specifically, Foucault stated that the technologies of the self allow subjects "a certain number of operations on their own bodies and souls, thoughts, conduct and way of being, so as to transform themselves in order to attain a certain state of happiness" (Porter *et al.*, 1989, pp. 153–4).

The regulation of the self insinuates a drive toward the self's protection from the precariousness of society, consequently suggesting a kind of disparateness from individuals and simultaneously dividing populations in terms of *us* versus *them*. In other words, the big data drive functions as a condition of possibility for the technology of the self to operate, thus creating a process of self categorization.

In addition, the big data drive does not merely name the drive toward BBD but the drive toward big data in a general sense. One significant consequence of this drive toward big data technologies is the way in which the drive affects the political realm, particularly in how political campaigns have become increasingly reliant on big data to provide detailed information on voters as a means to micro-target individuals. For instance, both the 2012 Obama and 2016 Trump campaigns used big data analytics in micro-targeting models. The Obama campaign explicitly "directed volunteers to scripted conversations with specific voters at the door or over the phone. Each of those interactions produced data that streamed back into Obama's servers", thus improving the data sets and "pointing volunteers toward the next door worth a knock" (Issenberg, 2012). Essentially, the Obama campaign used big data to predict who to talk to and to identify valuable individuals. More recently, Cambridge Analytica, a big data-mining company, has been at the center of the micro-targeting debate, as it profiles individuals to "personalise political messaging" (Privacy International, 2017). The debate is not necessarily about the success of the company to influence campaigns but about the profiling information provided about voters. Cambridge Analytica, for instance, collects information about individuals such as "your browsing history, your location data, who your friends are…" and uses these data sets to make predictions as to "what you're going to buy next, your likelihood to be female, the chances of you being conservative, your current emotional state, how reliable you are, or whether you are heterosexual" (Privacy International, 2017). These predictions are then provided to campaigns to aid in micro-targeting and influencing voter decisions. In retrospect, big data drive enables the subdivision of populations, and the entirety of a political campaign becomes based on who an algorithm predicts people will vote for. Big data drive is significant then because, as the drive perpetuates and pushes big data to the extreme, democracy becomes obsolete in a world where an algorithm makes decisions for people.

In short, as we witness a push toward big data technologies, the growth will only continue. Therefore, as big data evolves in general as a rhetoric, and we put more trust and confidence in it, big data drive is rhetorically significant because it names the operation that keeps the drive alive. Thus, big data drive provides a rational understanding of the drive and an understanding of the tensions within its discourse. Exposure and comprehension of the drive identify the fixation on big data as a rhetoric—as a potential inevitability rather than something that can be fundamentally challenged.

Acknowledgements

The authors would like to thank Amanda Axley and the editorial staff of the POROI journal for their extensive and generous comments and editing labor.

Copyright © 2020 Valerie Ortega and Kevin A. Johnson

Reference List

Airport Authority Hong Kong calls for closer collaboration as big data and biometrics projects advance. (2017 October). Future Travel Experience. http://www.futuretravelexperience.com/2017/10/airport-authority-hong-kong-reveals-tech-plans-and-calls-for-collaboration/

Baron, K., & Dorfer, S. (2015). *Fingopay: Visa tests finger vein payment tech*. Stylus. https://www.stylus.com/xhzdkd

Bengali, S. (2017, May 11). India is building a biometric database for 1.3 billion people – and enrollment is mandatory. *LA Times*. http://www.latimes.com/world/la-fg-india-database-2017-story.html

Biometric Center for Excellence (BCOE). (n.d.). *About the biometric center of excellence*. https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/biometric-center-of-excellence-1/about-the-biometric-center-of-excellence-1#:~:text=The-BCOE-is-the-central,laws-policies-and-regulations.

Biometric system and method for identifying a customer upon entering a retail establishment. (2003, January 23). FreePatentsOnline. http://www.freepatentsonline.com/y2003/0018522.html

Boyle, C. (2016). Pervasive citizenship through #SenseCommons. *Rhetoric Society Quarterly, 46*(3), 269–283.

Brill, J. (2016, January 5). *Privacy and data security in the age of big data and the Internet of things*. FTC. https://www.ftc.gov/system/files/documents/public_statements/904973/160107wagovprivacysummit.pdf

Carlson, B. (2010, July 3). Quote of the day: Google CEO compares data across millennia. *The Atlantic*. https://www.theatlantic.com/technology/archive/2010/07/quote-of-the-day-google-ceo-compares-data-across-millennia/344989/

Cox, M., & Ellsworth, D. (1997). Application-controlled demand paging for out-of-core visualization. *Proceedings of the 8th conference on Visualization*, 235.

Edkins, J. (2015). *Face politics*. Routledge.

Evans, D. (1996). *An introductory dictionary of Lacanian psychoanalysis*. Routledge.

Feinstein, D. (2013, October 13). The NSA's watchfulness protects America. *Wall Street Journal*. https://www.wsj.com/articles/SB10001424052702304520704579125950862794052

Foucault, M. (1977). *Discipline and Punish: The birth of the prison*. Pantheon.

Garvie, C., Bedoya, A., & Frankle, J. (2016, October 18). *The perpetual line up: Unregulated police face recognition in America*. Perpetual Line Up. https://www.perpetuallineup.org

Garvie, C, & Moy, L. M. (2019, May 16). American under watch: Face Surveillance in the United States. *Report of the Georgetown Law Center on Privacy & Technology*. https://www.americaunderwatch.com

Gates, K. A. (2011). *Our biometric future: Facial recognition technology and the culture of surveillance*. New York University Press.

Gunn, J. (2003). Refiguring fantasy: Imagination and its decline in U.S. rhetorical studies. *Quarterly Journal of Speech, 89*(1), 41–59.

Gunn, J., & Hall, M. M. (2008). Stick it in your ear: The psychodynamics of iPod enjoyment. *Communication and Critical/Cultural Studies,* 5(2), 135–157.

Hendrix, L. (2013, December 17). Biometric security poses huge privacy risks. https://www.eff.org/mention/biometric-security-poses-huge-privacy-risks

The history of fingerprints. (2020, September 29). Onin. http://onin.com/fp/fphistory.html

Issenberg, S. (2012, December 16). How Obama used big data to rally voters, part 1. *MIT Technology Review*. https://www.technologyreview.com/s/508836/how-obama-used-big-data-to-rally-voters-part-1/

Jagadish, H. V. (2015, November 16). *The promise and perils of predictive policing based on big data*. Phys. https://phys.org/news/2015-11-perils-policing-based-big.html#nRlv

King, R. (2015, December 1). *World's largest biometrics database leverages big data architecture*. Biometric Update. http://www.biometricupdate.com/201512/worlds-largest-biometrics-database-leverages-big-data-architecture

LaFrance, A. (2017, April 14). Amazon is making it easier for companies to track you. *The Atlantic*. https://www.theatlantic.com/technology/archive/2017/04/amazon-is-making-it-easier-for-companies-to-track-you/522999/

Lever, R. (2017, November 12). *Privacy fears over artificial intelligence as crimestopper*. Phys.org. https://phys.org/news/2017-11-privacy-artificial-intelligence-crimestopper.html

Lum, K. (2016, October 10). *Predictive policing reinforces police bias*. Human Rights Data Analysis Group. https://hrdag.org/2016/10/10/predictive-policing-reinforces-police-bias/

Lundberg, C. (2004). The royal road not taken: Joshua Gunn's "Refitting fantasy: Psychoanalysis, subjectivity and talking to the dead" and Lacan's symbolic order. *Quarterly Journal of Speech, 90*(4), 495–500.

Lundberg, C. (2012). *Lacan in public: Psychoanalysis and the science of rhetoric*. University of Alabama Press.

Lyon, D. (2002). Surveillance society: Monitoring everyday life. *International Journal of Urban and Regional Research, 26*(2), 429–31.

MacDonald, C. (2016, December 28). Researchers unveil lie-detecting robot kiosks that could help airports spot possible terrorists. *Daily Mail*. https://www.dailymail.co.uk/sciencetech/article-4071974/Researchers-unveil-lie-detecting-robot-kiosks-help-airports-spot-possible-terrorists.html

Mezzofiore, G. (2017, July 28). *This creepy technology can read your emotions as you walk down the street*. Mashable. http://mashable.com/2017/07/28/russia-facial-recognition-emotion-ntechlab-findface/#obUr7PH_.kqq

Myers, T. (2004). *Slavoj Žižek*. Routledge.

Neubauer, M. (2015, June 24). NYPD legal official on interplay of police technologies. *Politico*. https://www.politico.com/states/new-york/city-hall/story/2015/06/nypd-legal-official-on-interplay-of-police-technologies-097611

Nunns, J. (2017, September 21). *Pay with your veins – biometric payments arrive at Costcutter*. Computer Business Review. https://www.cbronline.com/news/verticals/fintech/pay-veins-biometric-payments-arrive-costcutter/

Pariser, E. (2011a). *Beware online filter bubbles* [Video]. TED. https://www.ted.com/talks/eli_pariser_beware_online_filter_bubbles

Pariser, E. (2011b). *The filter bubble: What the Internet is hiding from you*. Penguin Press.

Pokhriyal, N., Dong, W., & Govindaraju, V. (2015, June 2). *Big data for improved diagnosis of poverty: A case study of Senegal*. Brookings. https://www.brookings.edu/blog/africa-in-focus/2015/06/02/big-data-for-improved-diagnosis-of-poverty-a-case-study-of-senegal/

Porter, J. N., Martin, L. H., Gutman, H., & Hutton, P. H. (1989). Technologies of the self: A seminar with Michel Foucault. *Contemporary Sociology, 18*(1), 153–154.

Porway, J. (2014, September 6). *What is big data: Definitions from 40+ thought leaders*. Big Data Made Simple. https://bigdata-

madesimple.com/what-is-big-data-definitions-from-40-thought-leaders/

Privacy International. (2017, April 13). *Cambridge Analytica explained: Data and elections*. Medium. https://medium.com/privacy-international/cambridge-analytica-explained-data-and-elections-6d4e06549491

Rickert, Thomas. (2013). *Ambient Rhetorics*. Pittsburgh University Press.

Sanders, C., & Sheptycki, J. (2017). Policing, crime and 'big data': Towards a critique of the moral economy of stochastic governance. *Crime, Law and Social Change, 68*(1), 1–15.

Scientific American. (2014, January 1). Biometric security poses huge risks. *Scientific American*. https://www.scientificamerican.com/article/biometric-security-poses-huge-privacy-risks/

Sethi, A., & Bansal, S. (2017, July 19). Aadhaar gets new security features, but this is why your data still may not be safe. *Hindustan Times*. http://www.hindustantimes.com/india-news/aadhaar-gets-new-security-features-but-this-is-why-your-data-still-may-not-be-safe/story-RoZJAOUXtWZREr4V4M5TvK.html

Simanowski, R. (2016). *Data love: The seduction and betrayal of digital technologies*. Columbia University Press.

Simon, B. (2005). The return of panopticism: Supervision, subjection and the new surveillance. *Surveillance and Society, 3*(1), 1–20.

Sternstein, A. (2014, May 12). Is an expanded biometric immigration system worth $7 billion? *The Atlantic*. https://www.theatlantic.com/technology/archive/2014/05/is-an-expanded-biometric-immigration-system-worth-7-billion/362074/

Techopedia. (n.d.). *Biometric data*. https://www.techopedia.com/definition/26991/biometric-data

Timms, A. (2016, November 14). Is Donald Trump's surprise win a failure of big data? Not really. *Fortune*. http://fortune.com/2016/11/14/donald-trump-big-data-polls/

Trump, D. (2017, January 27). *Executive order protecting the nation from foreign terrorist entry into the United States*. https://www.whitehouse.gov/presidential-actions/executive-order-protecting-nation-foreign-terrorist-entry-united-states/

USA. (n.d.) Human Rights Data Analysis Group. https://hrdag.org/usa/

Violino, B. (2015, March 3). *Biometric security is on the rise*. CSO. https://www.csoonline.com/article/2891475/identity-access/biometric-security-is-on-the-rise.html

Waddell, K. (2016, April 8). How big data harms poor communities. *The Atlantic*. https://www.theatlantic.com/technology/archive/2016/04/how-big-data-harms-poor-communities/477423/

Winston, A. (2015, July 31). *Predictive policing is 'wave of the future' NY commissioner says*. Reveal News. https://www.revealnews.org/article/predictive-policing-is-wave-of-the-future-ny-commissioner-says/

Woodie, A. (2016, November 11). *Six data science lessons from the epic polling failure*. Datanami. https://www.datanami.com/2016/11/11/data-science-lessons-epic-polling-failure/

Žižek, S. (1997a). *The plague of fantasies*. Verso.

Žižek, S. (1997b). *The ticklish subject: The absent center of political ontology*. Verso.

Žižek, S. (1998). Cyberspace, or, how to traverse the fantasy in the age of the retreat of the big other. *Duke University Press, 10*(3), 483–513.

Žižek, S., & Daly, G. (2004). *Conversations with Žižek*. Polity Press.