The Report Committee for Kelly Michael Donovan
Certifies that this is the approved version of the following report:

ITEMS OF INTEREST AND WORDS OF POWER

APPROVED BY
SUPERVISING COMMITTEE:

Supervisor:

Bogdan Perzynski

Edwin Rifkin

ITEMS OF INTEREST AND WORDS OF POWER

by

Kelly Michael Donovan, B.A.

Report

Presented to the Faculty of the Graduate School of

The University of Texas at Austin

in Partial Fulfillment

of the Requirements

for the Degree of

Master of Fine Arts

The University of Texas at Austin

May 2014

Dedication

This report is dedicated to Kristy, for her love, perspective, and for being right alongside me throughout the program.

I would also like to dedicate this report to my parents, for their generous support, and their confidence in me.

Acknowledgements

I would like to express my appreciation to Bogdan Perzynski and Ned Rifkin. They have both been extremely valuable mentors throughout my graduate career.

I appreciate Bogdan for his patience, expertise and commitment. I appreciate Ned for his counsel, encouragement and enthusiasm.

I would also like to acknowledge Mike Smith and Dan Sutherland for their time and ongoing support.

Abstract

Items of Interest and Words of Power

Kelly Michael Donovan, M.F.A.

The University of Texas at Austin, 2014

Supervisor: Bogdan Perzynski

Kelly Michael Donovan is an M.F.A. Candidate in Transmedia in the Department of Art and Art History. Kelly Donovan creates artwork that examines our relationship to digital culture and technology, particularly the Internet. Following the global security disclosures in June 2013, Kelly Donovan created a series of work utilizing webcams, Internet search engines and a list of keywords used for monitoring social media to curate information and images relating to surveillance, privacy and national security.

Table of Contents

List of Figures

Introduction

For the last four years, my work has centered around my relationship to digital media, Internet culture, the Internet as a contemporary means of communication and its subsequent use to track those communications. Initially, the work depicted my immersion into the Internet and my involvement with online communities. I created video pieces using screen-capture software to record conversations with friends via the video-conferencing program, Skype. I worked with the webcam format. The screen-mediated experience became a canvas to create content. Elements such as: the browser windows on my desktop, the unpredictable quality of incoming video, and the laptop itself all became motifs in my work.

Inspired by my use of the webcam, I wanted to capture the instant content created from online video-chat communities such as Chatroulette and Omegle. Unlike Skype and other video-conferencing platforms, the format of these video-chat sites randomly pairs chat partners together, one-on-one, with the ability to converse through video, sound and text (Figure 01). The websites are often unmoderated, and give its users the option to switch to another randomly selected partner if they desire. I observed the role of the webcam on these sites and how it allowed users to be viewed and view others. In a previous body of work, I created a series of pieces comprised of live and recorded footage from Chatroulette.

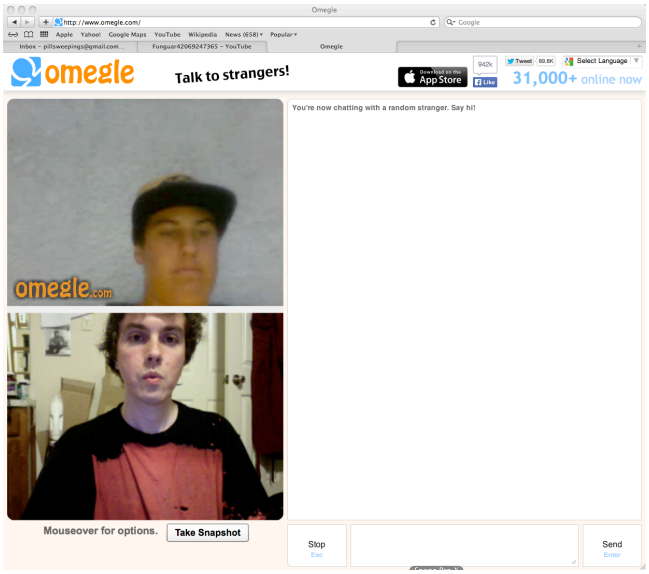

Figure 01: Screenshot of online chatsite Omegle.com

Saving and collecting content from online sources is a fundamental part of my daily practice. I collect images, meme-related content, videos, music, and articles I find interesting. At any one time, my Internet browser has up to sixty or more tabs open. I am unable to close these tabs because I might want to look at them later. I am not merely collecting random material, but rather archiving relevant information into a database. I frequent websites such as Facebook, 4chan, Piratebay, Youtube, various forums and other websites. Accumulating digital media is a cornerstone within many of these online communities. Vyshali Manivannan explains in "Attaining the Ninth Square: Cybertextuality, Gamification, and Institutional Memory on 4chan" that the aggregate of each users' database creates an "institutional memory" for that community (Manivannan 7). For many Internet users, the database exists as both a *personal archive* and *traceable lineage* of participation in an online community. While the creation of a database is both a private activity and part of a collaborative effort, it creates an Internet trail accessible to

anyone willing and capable of getting hold of it. This information can now be used in an official capacity to record users' histories. Like our friends following us on Facebook, Internet users are subject to their personal information, browsing habits, location data and messages falling under the scrutiny of third parties regardless of their intent:

> With digital records these harms are more acute. Once the data about our activities is gathered, law enforcement may keep that data indefinitely. They have a data hoard. That hoard grows with each new data request. Once created, the hoard can be continually rifled to investigate us but without any oversight. (Desai 2)

My practice collecting and curating digital material has transitioned my work from personal exploration to a wider investigation of online culture and surveillance.

My personal database of media is the result of long-term Internet use. However, my database pales in comparison to amount of intelligence government agencies mine and store. The Utah Data Center is a massive United States government data storage facility in Bluffdale, Utah. Journalist James Bamford from Wired Magazine explains,

> Flowing through its servers and routers and stored in near-bottomless databases will be all forms of communication, including the complete contents of private emails, cell phone calls, and Google searches, as well as all sorts of personal data trails—parking receipts, travel itineraries, bookstore purchases, and other digital 'pocket litter'. (Bamford 2012)

My laptop has about 400 gigabytes of hard drive space. Although sources vary, The Utah Data Center's storage capacity is estimated to hold billions of gigabytes (Hill 2013). I don't think it would be a leap to conclude that, like myself, these agencies store data for future evaluation.

Words of Power

In February 2012, responding to legal action under the Freedom of Information Act, The Department of Homeland Security (DHS) released a previously withheld document entitled Analyst's-Desktop-Binder. It contained guidelines and procedures on media monitoring that included a list of keywords compiled to help recognize "Items of Interest" (EPIC 2012). The compiled list of 374 words was created as a means to flag potential threats through various modes of communications. Spanning eight categories, these words range from various national security threats, to health concerns and natural disasters. Many of the words are rather pointed, directly implicating specific countries, regions and organizations, while others are more ambiguous.

I was not familiar with the Analyst's-Desktop-Binder and its key words at the time they were released. It was not until the mass surveillance disclosures[1] involving the National Security Agency (NSA) in June 2013 occurred, that I found information on the document, and that its contents, particularly the keywords, took on significance to me. My awareness of surveillance from my previous work made me realize how narrow my perspective was in light of the magnitude and severity the leaked documents implicated. I initially approached the list of search terms as "words of power." By cataloging these words through specific search criteria, the DHS imbued the key words with additional connotations beyond their own definitions. The DHS's intent behind creating the list of key words is to indicate behavioral patterns and even possible threats (DHS 20). The scope of the words potentially accuses nearly anyone as a threat. Many of the less overt

[1] An estimated 1.7 million classified documents leaked by ex-NSA contractor Edward Snowden

words come up in everyday conversations. Words such as: “snow”, “electric”, and “pork” (DHS 21). Outside of any context, using these words likely implicates the entire population. The DHS is essentially manufacturing threats as a result of the inclusion of so many everyday words. In Electronic Civil Disobedience and Other Unpopular Ideas, The Critical Art Ensemble noted, “there was growing paranoia among U.S. security agencies about controlling the electronic resistance. Oddly enough, these agencies scared themselves with their own constructions of electronic criminality” (CAE 19).

My work visually demonstrates that the Analyst’s Desktop Binder’s intent was flawed from the start. The emphasis placed on these words by the DHS exaggerates the actual threat the words pose, creating a positive feedback-loop like effect. Now, in addition to a quiet, behind-the-scenes rubric for monitoring citizens, these 374 words became components that influence behavioral patterns. In fear of being accused of illicit activities, people may censor themselves from saying or typing keywords from the Analyst’s Desktop Binder (Chambers 2013).

Conversely, their overuse and misuse in communications was proposed by some as a means of sowing confusion and disinformation within the government’s surveillance program as an act of defiance and subterfuge. When used by online pranksters, the claim was that the words could possibly disrupt the government’s surveillance program when used frivolously or in jest (Earle 2012). Websites such as “Hello, NSA” and “NSA Haiku” use simple sentence generators to create instant content suitable for spamming on forums, blogs and other social media platforms (Figure 02).

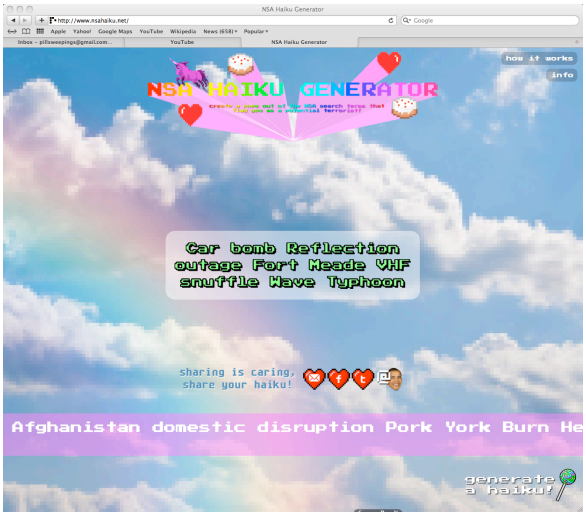

Figure 02: Screenshot of NSA Haiku Generator website

Based on the backlash created by these 374 search terms, I created a series of videos entitled “Words of Power (Spoken)” where I recite the words from each of the eight categories to emphasize their banality (Figure 03). By declaring the DHS’s terms in succession, with only the barest context besides their category heading, I aim to show the dependability of these terms to identify actual threats is preposterous.


Figure 03: Still from "Words of Power (Spoken)", 2014

I also created a complimentary video to address the idea of self-censorship and fear of using the DHS’s keywords (Figure 04). On video chatsites, users often angle their

webcams to keep their head out of frame as a way to hide their identity. I appropriated this simple technique while filming myself, and subsequently “beeped” out my recitation of the search terms. I contrast the direct declaration of the terms by staying safely anonymous and removing any instance of possible vocalized dissent.

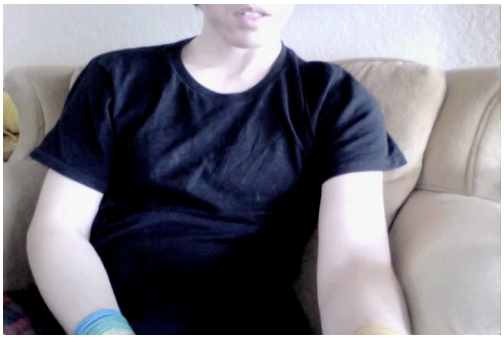

Figure 04: Still from "Words of Power (Censored)", 2014

My previous work centered on the premise of individuals watching and being watched through unprotected webcams (Figure 05). I wanted to expand my work to include the mass surveillance being conducted by the DHS and NSA.

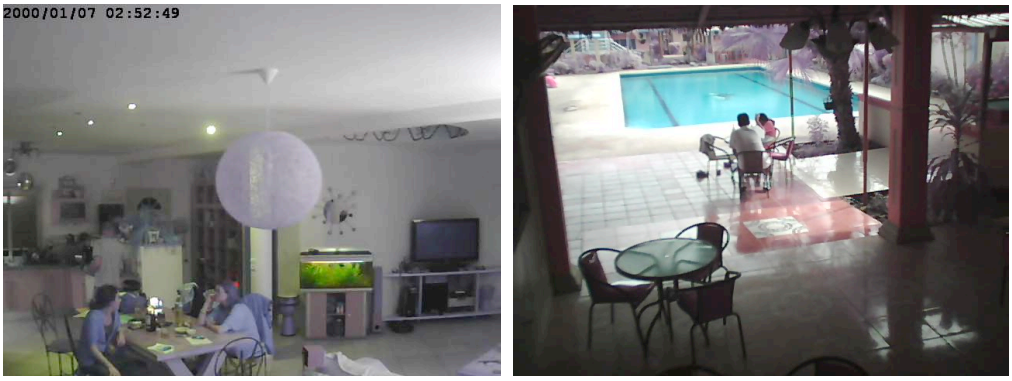

Figure 05: Examples of unprotected webcams

I continued to reference the visual language typical of webcams. The fixed camera angle, basic framing and inevitable compression artifacts all suggest the use of a webcam. The contemporary context of the simple and direct webcam format is universally understood

to Internet users. Although the webcam functions as a means of instant gratification for broadcasting oneself, it can be argued that Internet use alone implies consent to having ones' content followed, indexed, and scrutinized. As stated in Facebook Nation:

> The things we do and say online leave behind ever-growing trails of personal information. With every click, we entrust our conversations, emails, photos, location information and much more to companies like Facebook, Google and Yahoo. But what happens when the government asks these companies to hand over their users' private information? (Lee 152)

Using the online resources generally available to the public, I wanted to transpose my interpretation of the DHS's data collection processes and criteria.

Items of Interest

I began to think of the DHS search terms in the context of associated imagery. I wanted to know what images were being used to signify the public's preconceptions of these words. I repackaged the first search result of each word from the DHS's list into video montages using Google Image Search. In the videos, images of terrorists, disasters, death and gore share an indexical space with movie posters, political figures, government agency logos, and explanatory diagrams. What these montages create is a visual portrayal of Google users' interpretation of the DHS's concept of perceived threats. The "Report On Dangers And Opportunities Posed By Large Search Engines, Particularly Google" states:

> Google has become the main interface for our whole reality. To be precise: with the Google interface the user gets the impression that the search results imply a kind of totality. In fact, one only sees a small part of what one could see if one also integrates other research tools. (Maurer 16)

Google Image Search displays results filtered by file names, HTML metadata, surrounding body text, and ultimately page popularity (Brin, Page 1998). With this in mind, one can surmise that the first image best represents the ideology the word evokes in the mind of the public. Search engine results are malleable and in a sense "organic," because the image search results for each keyword portrays a veritable snapshot of public interests, fears, and topical information from the point in time the search was made. Based on this hypothesis, I repeated the image search six months after I first compiled this video series. Many of the first image results have changed (Figures 06, 07). The

theory that search engine results are ‘organic’ proves that the first image result depends on public interests.

Figure 06: First Google Image Search result for "Violence", October 2013 and April 2014 respectively

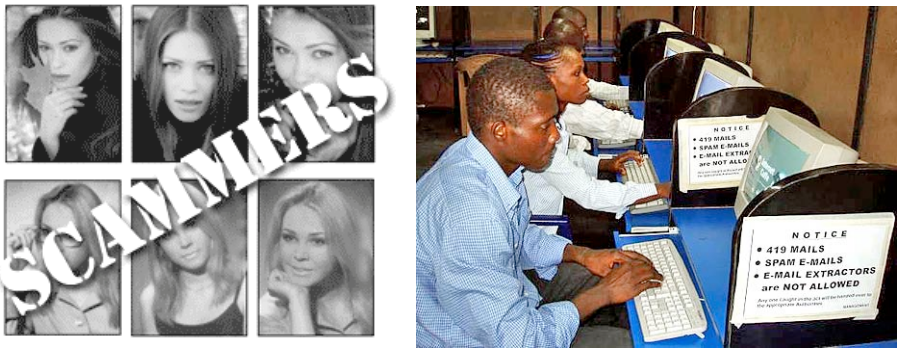

Figure 07: First Google Image Search result for "Scammers", October 2013 and April 2014 respectively

Latin America and the Middle East are two regions that are more heavily referenced or implicated by the Analyst’s Desktop Binder than other locations. From the United States’ geocentric perspective Latin America and the Middle East are depicted as places that harbor fear, violence and danger. For example, in the “Terrorism” category, countries such as Iran, Iraq and Afghanistan are listed along with terms like “car bomb”, “suicide attack” and “extremism” (DHS 23). Similarly, the “Southwest Border

Violence" category has Mexico and Columbia sharing space with "execution", "kidnap" and "shootout" (DHS 22). It felt appropriate to translate the search terms to the implicated regions' language. I did this to reframe the United States-centric worldview, to find out if the translated terms would present an alternative semantic vision through Google's lens (Figure 08). My intention for these videos is to highlight the relationship between the DHS's perception of threat and hostility versus Google's visual consensus on the search terms. I used Google's ability to organize a hierarchical system of perceptions and the DHS's ambiguous taxonomy to identify domestic threats to create a systematic visual arrangement highlighting their relationship.

Figure 08: First Google Image Search result for "Islamist" in Spanish, English and Arabic respectively, October 2013

In an earlier work from 2013, I displayed hand-picked images from books to online chat partners. I was interested in this process and wanted to advance this work. I broadcast the DHS image montages live on the video-chat site Omegle. Using "virtual webcam" software, I am able to replace my live webcam feed with video files or images, a similar tactic employed by advertising spammers on video chat sites. Because users can switch to a new chat partner at any time, the image set is broadcast without a clear indication of its associations or reasons for being grouped together. When I view the

broadcast from a third-person vantage point, I perceive an accentuation of the images' jingoism. My objective is to allow the represented DHS's search terms to mingle with the users of this international online community and highlight the connotations behind the words as viewed by Google users.

The DHS's search terms were created to monitor potential threats originating from the general populace. The Analyst's Desktop Binder outlines:

> Leveraging news stories, media reports and postings on social media sites concerning Homeland Security, Emergency Management, and National Health for operationally relevant data, information, analysis, and imagery is the first mission component. (DHS 4)

Responding to the DHS's actions, I have been compiling a list of words that I believe serves as the Analyst Desktop Binder's antithesis. The "Citizens' Items of Interest" I have gathered represent ideas, organizations and elements that could help citizens educate themselves about privacy, data mining, and mass surveillance. Words such as "corruption," "wiretap" and "drone" counterpoint the terms on the DHS's list. I applied the same process using Google Image Search with my series of "Citizens' Items of Interest," presenting the first result in the same manner as the DHS search terms.

The new keywords were compiled to empower citizens. However, the general public is ill-equipped to investigate events occurring covertly compared to the sophisticated proprietary software available to the government. Google Web Search is only as useful as its site index and permissible content. Google's "implied totality" and limitations restrict citizens' access to properly research and monitor government activities.

Post-Internet Influences

During the research and development of my work, I discovered several scholars and gallerists have begun calling digital artists working in the end of the 2000s part of a "Post-Internet" movement. Post-Internet art acknowledges that "Internet culture" is no longer a discrete presence, but rather something subsumed into culture at large. The process used by many affiliated with this movement is characterized as taking a "role more closely aligned to that of the interpreter, transcriber, narrator, curator, architect" (Vierkant 2010). Similarly, the work I have created re-contextualizes and reframes content acquired from the Internet to help viewers recognize associated imagery. Researching the "Post-Internet" movement has helped me more clearly define and focus the themes and process of my work. Jon Rafman's work, particularly his Google Street View project "Nine-Eyes," continues to influence my work and practice. His process for this project employs curatorial methods, for example, pulling content directly from Google Maps and choosing specific images as his final work (Figure 09).

Figure 09: Jon Rafman, image from "Nine-Eyes", 2009-Ongoing

Rafman's acknowledgement of Google as a source of raw material inspired me to approach it from a similar perspective. Oliver Laric's work has also become a significant influence. Laric annually re-creates a video piece entitled "Versions" (Figure 10). His

piece investigates the instability of images' authenticity in a culture of digital reproduction. Laric's work prompted me to consider how the DHS's search terms may be associated to the images I found on Google, and how the terms' relevance shifts within a continually changing contemporary cultural landscape.

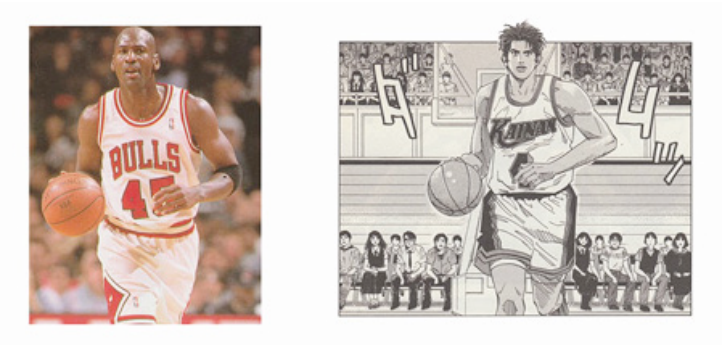

Figure 10: Oliver Laric, still from "Versions", 2012

During my research I found Emily Martinez's in-progress project "homelandsecurityhearts.us." It is similar to the "Hello NSA" website, but rather than creating content containing the DHS's search terms, Martinez proposes to code data-mining software that will pull posts from the social media site Twitter to locate the terms used in everyday contexts. I am excited to discover that a dialog is emerging among artists about the search terms and their significance. In terms of process, theme and content, I share similarities with each of these artists. I have used their work as resources to aid in my exploration of Google and the DHS's capacity to mirror culture.

Conclusion

The NSA surveillance disclosures are almost one year old and its contents are still trickling out of media outlets and into public awareness. There is no doubt that it will take citizens even more time to understand the full impact and consequences leaked in this disclosure. I believe there is a wealth of material to draw from for future work as the intelligence continues to be examined. On December 8th, 2013, a group of some of the most influential Internet-based corporations sent an open letter to the U.S. government asking for limitations on its surveillance program and data requisitions. In the letter published on reformgovernmentalsurveillance.com, these corporations make a bold statement:

> For our part, we are focused on keeping users' data secure — deploying the latest encryption technology to prevent unauthorized surveillance on our networks and by pushing back on government requests to ensure that they are legal and reasonable in scope. (Reform Government Surveillance 2013)

It has yet to be seen if the power these companies wield will reduce the government's ability to seize personal data. However, taking the notion of corporate personhood into consideration, there is now an emerging situation where a small group of corporations, acting as "people", are calling for legislative reforms that affect the use of personal information and the privacy of the populace. By using their services, Internet users, knowingly or unknowingly, give consent to these corporations to lobby their own interests in the legislative process. Internet users must continue to weigh the benefits and hazards of corporations like Google. On one hand there exists enormous potential for collaboration and communication, but it shares the same space with an increase in

surveillance and domineering corporate ethics. If government agencies such as the NSA and DHS are compelling companies like Google and Facebook to disclose their users' personal data, what does that say about the surveillance and data collection these companies are performing?

There is no stated right to privacy in the U.S. Constitution (Things That Are Not 2010). The USA Freedom Act (S. 1599: Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection, and Online Monitoring Act) was submitted on October 29, 2013 to a congressional committee by Congressman Jim Sensenbrennar [R-WI] and Senator Patrick Leahy [D-VT]. The Act's purpose is:

> To rein in the dragnet collection of data by the National Security Agency (NSA) and other government agencies, increase transparency of the Foreign Intelligence Surveillance Court (FISC), provide businesses the ability to release information regarding FISA requests, and create an independent constitutional advocate to argue cases before the FISC. (USA Freedom Act 2013)

However, as of January 9th, 2014, the bill has only been submitted to three House committees and the Subcommittee on Crime, Terrorism, Homeland Security, and Investigations. The USA Freedom Act cannot be enacted until it passes both the Senate and the House, and signed by the President. Based on statistics from govtrack.us, the bill has a 36% chance of passing the House (H.R. 3361 2013) and only a 10% chance of being enacted by the Senate (S. 1599 2013). Between 2011-2013 only 3% of bills brought to the Senate have been put into law (S. 1599 2013). Even if just parts of The USA Freedom Act are made into law there is no guarantee on how quickly it will be executed or its long-term efficacy. Considering the increasing role of the Internet for social networking, research and entertainment, the thought of "opting out" from using many

online services is impractical for most people at best, and at worst, impossible. Even after someone has deleted their profiles and shut down their accounts, the trail of data left behind still remains and may never disappear (Goldstein 2014). The only secure method to limit the access to personal information right now is to take measures in reducing ones' digital footprint. As an artist who has formed their practice around the Internet and its use, I do not advocate a fearful rejection of technology. Internet users can take a pro-active role in limiting the amount of their personal data that is freely accessible for consumption, and decide which services they want to use and in what capacity. It is my wish that my work contribute to the growing dialog surrounding issues regarding privacy and surveillance related not only to the U.S. government, but Internet service providers and online companies as well.

Bibliography

Brin, Sergey, Lawrence Page. "The Anatomy of a Large-Scale Hypertextual Web Search Engine." 1998. Web. Retrieved from http://infolab.stanford.edu/pub/papers/google.pdf

Chambers, Chris. "NSA and GCHQ: The Flawed Psychology of Government Mass Surveillance." *The Guardian,* 26 August 2013. Web. http://www.theguardian.com/science/head-quarters/2013/aug/26/nsa-gchq-psychology-government-mass-surveillance

Critical Arts Ensemble (CAE). *Electronic Civil Disobedience and Other Unpopular Ideas*. New York: Autonomedia, 1997. Print.

Department of Homeland Security (DHS). *Analyst's Desktop Binder*. 2011. Retrieved from http://www.scribd.com/doc/82701103/Analyst-Desktop-Binder-REDACTED

Desai, Deven R., "Constitutional Limits on Surveillance: Associational Freedom in the Age of Data Hoarding" February 27, 2014. Web. http://ssrn.com/abstract=2404782

Earle, Grayson. "NSA Haiku". 2012. Web. http://www.nsahaiku.net/

"EPIC v. Department of Homeland Security: Media Monitoring." *Electronic Privacy Information Center,* 2012. Web. http://epic.org/foia/epic-v-dhs-media-monitoring/

Goldstein, Jessica. "Meet the Woman Who Did Everything in Her Power to Hide Her Pregnancy From Big Data." *ThinkProgress*, 29 April 2014. Web. http://thinkprogress.org/culture/2014/04/29/3432050/can-you-hide-from-big-data/

Hill, Kashmir. "Blueprints of NSA's Ridiculously Expensive Data Center In Utah Suggest It Holds Less Info Than Thought". *Forbes,* July 24, 2013. Web. http://www.forbes.com/sites/kashmirhill/2013/07/24/blueprints-of-nsa-data-center-in-utah-suggest-its-storage-capacity-is-less-impressive-than-thought/

"H.R. 3361: Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection, and Online Monitoring Act". 2013. Web. https://www.govtrack.us/congress/bills/113/hr3361

Lee, Newton. *Facebook Nation*. New York: Springer Science+Business Media, 2013. Print.

Manivannan, Vyshali. "Attaining the Ninth Square: Cybertextuality, Gamification, and Institutional Memory on 4chan". October 10, 2012. Web. http://www.enculturation.net/attaining-the-ninth-square

Maurer, H . "Report On Dangers And Opportunities Posed By Large Search Engines, Particularly Google". 2007. Web. Retrieved from http://www.iicm.tugraz.at/Ressourcen/Papers/dangers_google.pdf

"Reform Government Surveillance". 2013. Web. http://reformgovernmentsurveillance.com/

"S. 1599: Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection, and Online Monitoring Act". 2013. Web. https://www.govtrack.us/congress/bills/113/s1599

"Things That Are Not In the U.S. Constitution". 2010. Web. http://www.usconstitution.net/constnot.html

"USA Freedom Act". 2013. Web. http://sensenbrenner.house.gov/legislation/theusafreedomact.htm

Vierkant, Artie. "The Image Object Post-Internet."2010. Web. http://jstchillin.org/artie/pdf/The_Image_Object_Post-Internet_us.pdf