The Breach:
An infiltration of user privacy

By: Taehwan Lee

Bachelor of Fine Arts in Illustration
Rhode Island School of Design
June 2018

A thesis submitted in partial fulfilment of the requirements for the degree of

Master of Fine Arts, Communication Design
School of Design
Pratt Institute
May 2020

The Breach:
An infiltration of user privacy

By: Taehwan Lee

Received and approved:

Lead Thesis Faculty Prof. Tom Klinkowstein, May 2019

Thesis Resource Advisor Corwin Green, May 2019

Chairperson Santiago Piedrafita, May 2019

MFA Thesis Candidate
Taehwan Lee, May 2019

Table of Contents

Thesis Question

In what ways can business models of Search Engines expose users’ private information? Where? How?

How can we update the current Data Protection Regulations to improve data management and secure sensitive user data?

Abstract

Business models of search engines such as Google's are designed so that users believe they are offered a library of infinite resources. As users search up their desired content, their search history data are stored online and observed by corporations, in which they bid on advertisements to publishers that have the desired user demographics; as a result, users will frequently encounter advertisements that relate to their interests. The moment users' search data is utilized by enterprises, a concept called the breach occurs, which is an opening in an online business model that allows corporations to observe and utilize stored user data to promote related businesses. The breach is possible due to the convenience of search engines and internet platforms, which is known as the bait.

Privacy is a recurring issue with the relationship between online search algorithms and users worldwide because data leaks during a breach can expose private information about users such as addresses, credit card information, or personal photos. As a result, regulations such as the General Protection Data Regulations in 2018 are implemented to address the issue; while the GDPR ensures user data is secure during a breach, the risk of data leaking through a breach is still possible, so how can the current Data Protection Regulations be updated to improve data management and further decrease the possibilities of data breaches?

Glossary

1. Data
    - Information about a user stored on the internet. This can be through social media, emails, or any site on the internet.
2. Privacy
    - A condition where the user is free from being observed or disturbed.
3. Form
    - An arrangement of elements (ordering, pattering, shaping) that bring together a greater whole.
4. Whole
    - Combination of forms that bring together a final product/strategy that is marketed (can be successful or not) to users. Includes the forms of design such as message, tone, etc.
5. Business Model
    - An example of the whole. This is formed through the symbiosis among users, publishers, and businesses.
6. Consumers/Users
    - The form that serves as the backbone which allows online business models to thrive. They consume contents, which is stored as data for corporations.
7. Bait
    - Something that entices the user. It is a lure to a breach created by publishers.
8. Publishers
    - The form that provides online content for users to exchange their data for.
9. Corporations
    - The form that is responsible for symbiosis with the publishers through keyword monetization and advertisements.
10. Breach/Leak
    - An opening that allows user information to be extracted for the benefit of corporations. This is the result of bait.

Introduction

When Google was founded in 1998, the world has witnessed the world change through the rise of a new industry. The internet allowed interaction with multiple resources and services simpler such as Google Maps nullifying the need for paper maps or Uber serving as a "private taxi" that would arrive on the user's command anytime and anywhere. So why is the internet successful in what it does? That is the genius behind the concept behind smartphones; the designers utilized the design theory term Affordance in Levine's "Forms, Rhythm, Hierarchy, and Network," which is used to describe "the potential uses or actions latent in materials and designs," so that internet interactions have a versatile interface, capable of being used in multiple ways. Each internet user in the world has its reasons for interacting with the internet, so it has to accommodate the variety of people by being very versatile in how it can interact.

Literature Review

The anatomy of the internet can be interpreted through Caroline Levine's concepts in "Whole, Rhythm, Hierarchy, Network." Levine starts in her book by describing a concept called the form, which is a base structure of the design. In itself, it is a very limiting structure due to whatever niche it favors. However, that is where the second component called the Whole takes place. The concept of the whole is a number of forms that converge together, creating a more flexible and versatile system that is easier to interact with. We can interpret the whole as the internet or more specifically the world's most known search engine in the world, also known as Google. The forms, on the other hand, are what is accessible through Google such as social media, emails, personal websites, etc. One of those forms have a more transparent limitation or niche, but when these forms are combined, their versatile potential is endless. As mentioned previously, Levine emphasized on the concept of Affordance, which is "the potential uses or actions latent in materials and designs." One of these forms in question has a large degree of Affordance, but the whole of the internet is seeming with Affordance. As a result, the future greatly favors the internet due to how versatile it is designed to function.

With this in mind, we ask how does the internet whole utilizes the form to be more convenient for each user? Every search the user goes through is data stored for search algorithms to find content similar to the user's interest. This is a form that also allows companies to send advertisements to certain audiences. For example, if the majority of my Google search history is focusing on luxury car brands, then I will be more likely to find ads related to different car brands. This concept consists of three forms, known as the users, businesses, and the publishers, that make a triangle called the Google business model. The users utilize Google's search engine, which allows better data of proper keywords for businesses. The businesses take the keywords and pay the publishers to produce more content in exchange for targeted ads to the proper audience. The publishers monetize their content and continue to provide free content for users to consume.

Since this sounds very convenient to all parties involved, what seems to be the issue here? The primary issue is the potential risks of storing information on the internet. In many cases, very sensitive information can be stored on the internet that can be used for really harmful purposes if put into the wrong hands. These situations are known as data breaches. When a data breach occurs, the users and the publishers suffer greatly as a consequence. One notable example is the data breach of Adobe in 2014. Some hackers got into Adobe's database and leaked thirty-eight million users' IDs and passwords. To make things worse, three million of the thirty-eight million also got their credit card and login data stolen from them. As a result, many users lost vital information and Adobe paid over one million dollars in legal fees. When we store our data to the internet or sites, we place our trust in the publishers that our data will be protected, but there has been extreme doubt of the safety of our information due to the neglect of our data.

For example, in 2016, the well-known application for private rides known as Uber was hacked by a group of people, who were able to get not only sensitive information from users but also from drivers such as their license plate. Fifty-seven million users and six hundred thousand drivers were affected by this incident. According to an Wired article by Andy Greenberg, this breach was ongoing for a year until this incident went public. During this year, Uber tried to keep this incident quiet by bribing the hackers with hush money. Naturally, Uber has received a lot of criticism due to how lightly users' information was being treated and how they tried to bribe the ones responsible for exposing millions of users' private information. Simply put, with many of these incidents occurring, it is natural for internet users to be wary of storing their private information on the web because there is a risk it can be exposed like the previous incidents mentioned. As a result, laws such as the General Data Protection Regulation or protection programs like VPNs have arisen to help protect users' data from being breached. These are the right steps to provide protection to the users, but there is one dilemma that is being overlooked.

When data is breached, more severe consequences can occur depending on the information being leaked. Paul Chan at the Los Angeles Review of Books stated: “as the soul, our data is abstract and disembodied, and it will go on existing after we die.” When a breach occurs, the private information leaked can be accessible to other users. So even if the user works with publishers or businesses to patch up the breach, the chances of new breaches will open up in the form of reuploads and reposts.

For example, Safiya Umoja Noble reported on page 280 in “Algorithms of Oppression” that on March 9, 2011, a “St. Louis high school teacher's past exotic dancer work in the pornographic industry in the 1990s was discovered and leaked to the students of St. Louis. While the teacher tried to dispose of all that data on the internet and said those were “one of the greatest regrets in her life,” school officials found her unfit to be a role model for students despite her working in that school for two decades and fired her. As shown through this example, internet data from decades ago can be unearthed to haunt the victim once more and potentially ruin lives. Manually deleting files or clearing cache does not permanently remove all traces of data users do not wish to see, especially if it has been breached to others previously. This is why websites such as IsAnyoneUp.com started harmful breaches in 2010 such as “sexually explicit images of people that included their name, address, and social media profiles.” Revenge porn is one of the harmful effects breaches caused. As one victim states on page 283 of Algorithms of Oppression, “I am a disgrace to my family. My self worth has gone out the window and I worry I may never get it back. This keeps me one step away from happiness every single day. I don't know what to do anymore.” Fortunately, regulations for breaches like revenge porn have been regulated such as the founding of the Cyber Civil Rights Initiative and the first revenge porn law formed in California on December 4, 2015.

Noble states in “Algorithms of Oppression” on page 285 that “one’s past is always determining one’s future because the Internet never forgets.” When one has sensitive information breached without consent or makes a mistake the user immediately regrets after, these breaches can harm the victims severely, even take lives. One example is through a famous YouTuber known as Etika, who cried pleas for help over his mental stress of being monitored by viewers as a public content creator. Many of his viewers did not take his pleas seriously and ridiculed him through retweets and videos. As a result, his body was found on the East River on June 24, 2019. His death was through drowning and suicide. Overall, while breaches are primarily used to make interaction convenient between users and the internet, these breaches still have the potential to harm users severely.

Levine mentioned in Page 9 of her book that internet users are “concerned with breaking forms apart that we have neglected to analyze the major work that forms to do our world.” Publishers of search engines, social media, or anything data storage related may not be innocent as we believe them to be, but they are an essential form that contributed to the modern culture we live in. The more regulations and protections that are being regulated into these corporations, the more difficult it will be to provide content for the users. For example, in an experiment where the Facebook business model was dissected so one side of the triangle was gone and simulated the results of the missing form, every side removed for each test led to the same result. Businesses would have to guess what ads are appropriate to throw at certain audiences, which will be very inaccurate, and more money would be spent on corporations to keep their company afloat rather than focusing on creating new content or features for the users. That doesn’t mean wanting to protect your data is being selfish and causing corporations to lose money, but in the end, this is a tradeoff that needs to be concerned when going through data protection regulations. Basically, this is a debate that users and corporations need to address to figure out what is the appropriate step to move forward in. Easterling said in "Medium" that, "there is no growth or ideation without argument or debate." Finding that proper compromise is no easy task and the most practical way to accomplish this is through years or even decades of debate on what is the best approach to take. There will be a struggle and there will be hardships to reach that destination. Marc Hazzenhaul, a professor of User Experience and Ergonomics, the experience is more important than the final product because the process defines the structure of the product, which connects everything so that it is sturdy. Only then would all parties understand and agree on the ideal compromise.

Overall, finding the appropriate first step for this is not easy. Analyzing the business models of search engines and referencing data breach incidents let me to the conclusion that rather than search for a concrete solution, it is best to contribute to the situation by pointing out suggestions to the parties involved so that they will be potential forms that can contribute to reshaping the ideal form that will guarantee efficiency and safety for both users and corporations.

Historical Framework

The idea of data leaks as understood today is a relatively new concept. Since the advent of the internet, we can easily list examples of data leaks. However, leaks are present in history as phenomena in which information infiltrate into or from a system; we can interpret diseases as forms of information.

Before we can discuss leaks, we need to address business models to the concept of leaks.Until the end of the 1800s, the primary business model was utilizing trade, a simple concept of giving something in exchange for another, such as the Silk Road or Triangular Trade routes during American Colonization. According to ushistory.org, the main leaks in the trade era are primarily privacy, smuggling and disease. For example, when Britain increased the taxes towards trade in the American colonies, it encouraged traders to resort to smuggling to avoid being unfairly taxed. Overall, each of them are caused by a group of individuals who created a hole in the system that temporarily shut down the functionality or full optimization of the system.

In the 1900s, the Production era emerged, which focused on quantity over quality such as factories, which were made to mass produce objects despite their low quality. There are instances in previous business models where regulations managed to resolve the breach significantly. For instance, the Great American Fraud during the Production Era perfectly describes a scenario of a leak and a regulation. In the early 1900s, many businesses began to make false claims that some drugs have benefits to the human body or can cure conditions like cancer. As a result, many consumers didn’t know better and purchased drugs such as cocaine and took them, unaware that they have not only been lied to, but will end up being addicted to these drugs. To make things worse, some customers died due to drug overdose without them realizing. Another example of the Great American Fraud is through the Coca Cola company, where small bits of cocaine have been mixed in with their soft drinks without the consumers’ knowledge. The cocaine made the drinkers want to continuously buy more products and made more money for Coca Cola. These incidents have increased out of control and as a result, the Food and Drug Act was implemented in 1906. This act banned the sale of poisonous and lethal potent medicines. This regulation evolved into the Federal Food, Drug, and Cosmetic Act when more leaks after the act have surfaced.

In 1931, the Marketing Era caused sellers to focus on Market Segmentation and how to be a unique business. This era continued to evolve into variations, such as the Relationship Era, which utilized the Marketing Era, but added a new factor which is utilizing long term customer relationships. When new technology arose during the Marketing era, so did new forms of the breach. For example, when the telephone was invented during 1876, many callers received a series of robocalls, which are known as the use of recorded or artificial voice for sales voice. Since these robocalls have been disruptive to many telephone users, laws such as the Telephone Consumer Protection Act of 1991 have been implemented to allow victims of robocalls to fight back against these frauds. These robocalls still continue to be a nuisance when cell phones and smartphones have been created.

Another example of the breach through modern technology is when television ads were normalized starting 1941. Ever since then, there have been underhanded ads that subtly take advantage of the innocence of children such as broadcasting ads related to a television show of interest right after that show is in a commercial break. It brainwashes children to buy a product because it uses television shows children are interested in. As a result, Peggy Charren, an activist, founded the Action for Childrens’ Television, which is known to prevent corporations from creating commercial abuse to children television. This act was created because children are more gullible than adults and are unaware they are a leak corporations can abuse through tempting advertisements. She created the Children’s Television Act of 1990, which regulated businesses to control the content of advertisements on certain times of television to avoid overinfluence. This act has been a successful regulation towards children during the time, but the internet has made a new leak to allure children such as online merchandise stores YouTubers advertise in children content. Over time, there will be a regulation to hold back the amount of advertisements made to take advantage of children and then a new leak through a different format will arise. Overall, all these leaks have one common theme. They take advantage of gullible consumers and attempt to scam them into purchasing a faulty product or a product that they don't need. The primary difference is that they are all accomplished through different formats.

Over time, these business models arose to the New Year's Model, which is the current model we are utilizing. It is a hybrid of the Marketing Era and the Relationship Era, but introduces the internet and crowdsourcing as other options to make businesses flourish. The internet is the main resource for allowing The New Year's Model to thrive, which leads to the breaches corporations and unwanted third parties cause to users. For example, in 2016, a small group of hackers managed to steal the database of fifty seven million users from the application Uber and seven hundred thousand license information from drivers. What made this breach more scandalous is that Uber has known this incident was going on for a year and was trying to bribe the hackers to give back the information subtly to keep the public from knowing this happened. According to Andy Greenberg in a Wired Article about the incident, Uber was criticized harshly for being irresponsible with data from its users. Overall, users have a good reason to be wary of giving out data to corporations if some corporations are willing to treat user data without any care such as Uber.

Throughout analyzing the different eras of business models, we can conclude that leaks have occurred throughout history. It has only become digitized through the rise of the internet.

Delimitation

For a start, this thesis is not looking for a solution or finding a perpetrator to blame for this predicament. Society may be able to patch the breaches going on in the internet, but they are only temporary. The breach has occurred throughout history in the form of exploits and only became digitized because the internet is the future. Since we still haven't found a solution, we will have to accept that this is an unfixable issue. Since there is no real solution to this global issue, there is no point in looking for a solution.

A common misconception is that corporations are to blame because they have the power over consumers' data and their negligence caused most of these issues. However, the ones who truly benefit from causing this mayhem are select consumers who harm all three aspects of data traffic for self-gain. For example, Uber may be responsible for being so careless with its data, but shouldn't we look at the hackers who held the users' data hostage? Uber was a victim and tried to keep the issue subtle to avoid panic. It wasn't the best approach, but they considered their users' data while negotiating with them.

When third parties are involved in disrupting data traffic, it isn't fair to blame anyone because all three parties are involved. Rather than find someone to blame or a solution, the best we can do is educate the public about data traffic and how they can protect themselves.

Contribution Statement

The breach is an opening in an online business model that allows user data to be stored and accessible on the internet to be utilized by corporations to promote related content. Online business models for internet engines are designed to be simple and beneficial to both users and corporations so that the breach happens subtly. For example, Facebook's business model is run by a hidden revenue generation where "over 98% of Facebook's revenue systems came from targeted advertisements shown on the feed." The feed is Facebook's method of utilizing the breach by ranking content from friends, groups, pages, and advertisements in an endless scroll. Firstly, Facebook provides free data to users to collect data for their algorithms. The data stores are sold as targeted ads to businesses to the feed. Businesses pay Facebook ads based on how well they do such as 'Likes,' 'Clicks,' and 'Shares." These targeted ads are then provided to users so that the chances of these targeted ads doing well is very high. Overall, this becomes a tight loop shown as a triangle-shaped business model where data collection is the primary resource for making search engines and social media on the internet thrive. For example, if a user is interested in cars and spends most of his or her time looking at car models in the feed, the algorithm will understand and businesses will send car ads to the user because that is what the user seems to be interested in.

In a former experiment, a fourth point in the Facebook triangle business model called the regulation aspect was implemented. A regulation is known as a set of rules to counter a breach. For example, the General Data Protection Regulation of 2018, also known as the GDPR, is a regulation to ensure data is being handled properly between publishers and businesses because data breach instances that leaked personal information from users such as the eBay cyberattack of 2014 were very common. In this updated Facebook business model, the advertisement bid from data collection needs to be regulated and filtered so that it ensures the breach isn't abusing the user's private data and minimizing the chances of personal data leaking out. Another part of this experiment is to remove one side of the business model triangle and simulate what will happen with this extraction.

Overall, the two experiments have similar results. Removing a side will break the feed, resulting in showing advertisements that users are not interested in, thus losing money for the search engine corporation and the advertisement company. While the business rhombus is not as destructive as removing one side of the triangle, advertisements will have much more difficulty going through the regulation, resulting in fewer ads being distributed to the users, thus losing money for both the search engine corporation and the advertisement company. What will these scenarios result? The main downside is corporations will have to spend more money keeping their company afloat rather than focusing on new contributions to progress the internet further. While users may be wary of privacy issues when surfing on the net, many people seem to be content with these due to the convenience they provide in exchange. For instance, in a survey of twenty people in a college, the vast majority of them are aware of these issues with data privacy but don't really consider them a threat much due to convenience and VPN being a secure line of defense for them. With these experiments, I had to question myself how will a regulation truly benefit internet users? It can be argued that it provides a line of security for non-VPN users, but that counterargument is discriminatory towards users who put effort into securing their privacy. Of course, that doesn't mean users who can't afford security don't deserve them, but it will be unfair to not only those who put the effort to secure their privacy but the VPN companies who put the effort into giving users the chance to secure their privacy further. Overall, this contribution will not only affect corporations related to data privacy but the majority of internet users who care about their privacy being breached online. With this in mind, how can we find a solution where both corporations and users can benefit?

One of the primary target groups that will be changed for the better with any potential "solution" are those who became infamous through negative exposure. Those individuals are referred to those who didn't consent to have their information leaked, but got their information leaked due to individuals leaking it, causing problems to the victims. One of the bigger examples of these is through revenge porn, which are sexually explicit photos or videos of a person being posted online, ruining the person's reputation and professional life. In page 283 of Safiya Noble's Algorithms of Oppression, it describes how a person's life can be ruined when these embarrassing pieces of information are leaked to the public, which can lead to the individual refusing to go outside to family members rejecting the victim as part of his or her family. One of the websites infamous for posting revenge porn is IsAnyoneUp.com, which was created in 2010. It not only allows explicit content to be posted there but also the victim's social media profiles such as Facebook or Twitter. In 2015, there have been efforts to deal with this issue such as the Cyber Civil Rights Initiative. The number of these incidents may have reduced significantly due to new laws, there must be new ways to update these laws because there are still more of these incidents that must be dealt with. It may be impossible to sever a leak when it gets posted because the internet will continue to repost content infinitely. One example of an attempt to censor a leak is through the 2018 suicide forest incident, where a YouTuber named Logan Paul posted a video broadcasting a guy that committed suicide. The video showed disturbing details about this dead person such as how purple the victim's hands were. While YouTube tried to remove any video related to the incident, YouTube was unable to stop the angry users who want to spread awareness of how insensitive Logan Paul was for posting that video. Overall, this shows two cases on the moral conflicts of regulating the internet further. In one case, it provides security to incidents that can non-consensually ruin peoples' lives. On the other hand, it will provide exposure to address how certain user’s actions on the internet will receive backlash if the content was very insensitive and immoral to viewers.

Overall, there are different types of users and corporations that will be affected by attempts of regulations on the internet. The main issue being addressed is how there will always be a group that will receive the short end of the stick when a decision on how to deal with privacy and data storage is made.

Process and Methodology

My process and methodology consists of a series of experimental projects that my capstone proposal took inspiration from. From the start, the concept and components of a breach has been difficult to convey in words because of the complexity of the topic, so imagery was used to make explaining the topic simpler. One of the first examples was through analyzing and altering the business models of search engines and social media. One example is through the Google business model. In the original Google Business Model, which is also known as the hidden revenue business model Google based on its algorithm success, it was designed in a triangle business model that undergoes a cycle among three forms: the publishers, the users, and the businesses. The publishers provide free content to the users, which attracts them to use Google’s search engine. Based on what was popular in users’ search engines, businesses bid on keywords to be monetized so that both publishers and businesses will be able to make more money through the user's clicks. This triangle cycle leads to users receiving the desired free content while publishers and businesses make a profit. However, in between the cycle, there are hidden details Google left out that affects the users. In the transfer of free data from Publishers to Users, the free data is a form of bait to lure users in to allow the breach, which is the side between the users and the businesses. Utilizing the breach is then shown on the side between businesses and publishers. Overall, the model shown describes the honest depiction of how data is being transferred among the three forms of the triangular business model. I continued to make a series of these business model depictions based on other search engines and social media to see how other companies and publishers create this form of data extraction among users. Many of them utilize the bait but alter how it is being used so it is effective to users.

The next phase also named the 3-D business model, is by converting the triangle business models into three-dimensional. The triangle model has been layered so that the three factors responsible for the “hidden revenue generation,” also known as ‘users,’ ‘businesses,’ and ‘publishers,’ are on separate triangles. The triangle shapes are being supported by other chipboard pieces so that they stay elevated. Through this model, the users are no longer part of the business model loop, but the pieces keep the model staying up. Corporations such as Google are only able to stay stable through the interaction of users. If the users are the supporting pillars, then what is the vacant triangle in the model? The remaining triangle is actually the primary business in this business model. The ‘business’ side of the loop can actually be divided into two categories: the primary business that started keeping this cycle running and the corporations that wish to create a symbiosis with the primary business by bidding on advertisements. In short, publishers create content that is beneficial to the primary corporations that attract the attention of other businesses that bid for keywords to monetize the targeted publishers. Behind the scenes, the users are the backbone that keeps this system alive.

Like the series of business models in the first phase, I created another series of business models in a three-dimensional setting to reinterpret how the powers among the three forms of a business model can be portrayed differently.

The next physical model after the 3-D business models is focused on analyzing the importance of certain information compared to others. This model describes the data from a user, which is divided into five layers: the interface, social media, work information, home information, and personal information. The layers are stacked on top of each other so that more personal layers such as home information and personal information are below less private information such as the interface and social media. Sections of each layer were laser cut so pieces can be removed from them. Underneath each cut piece, there are pieces of user information that only get more personal the deeper one goes. A user can use tweezers to extract these pieces to get information out. To get private information out of a user, one has to dig deep into the layers of user data. This model shows how corporations and unwanted third parties extract stored information out of users. They do not dump out the information but extract it delicately so that it isn’t easy to notice. However, users will be able to know their data is tampered with because sections of data from the layers are either removed or moved around. The severity of tampering can be shown by how deep the corporation or third party went into the layers of user data. For example, the victims from the Uber hack scandal in 2016 experienced sensitive information such as drivers’ licenses and ID numbers. Through the model, this is a breach of users’ work information, and personal information, which are the deep ends of user privacy. As users worldwide become more involved with the internet, their identities are being compressed into layers of data like how the human body functions. Like the human body, it needs to be taken care of so unwanted parasites do not invade and disrupt sensitive information.

Overall, for the breach to be described through design or models, it needs to show the key components responsible for this issue such as how corporate business models work or how user information can be extracted by unwanted guests. As each model unravels each layer that brings the breach together, perhaps an opening that shows how to dismantle it will show itself.

Capstone Proposal

My capstone proposal consists of a series of objects that will describe the elements that make up a data breach in a simpler and more digestible way. The reason for working on this capstone proposal is because describing the breach is very complex through text or word. The more practical method to describe how the components of a breach works are through imagery and symbolism.

The series will be focusing on the topic of Benjamin H. Bratton's "The Stack: On Software and Sovereignty." The stack consists of six layers that make up how data is composed of the world. The six layers are called the User, Interface, Address, City, Cloud, and the Earth. Originally, Bratton describes the layers of the stack that each layer serves as a component for a greater whole weaved together by multiple systems. Bratton explains that as long as we can understand how each layer of the Stack works, it can serve as a key to reprogram the greater whole to be a better place. I believe Bratton's work serves as a reference in explaining how a data breach works since a breach interrupts the symbiosis publishers, consumers, and corporations serve. If we interpret what role each Stack layer serves in the greater whole of data management, we should be able to understand the significance of data breaches. After interpreting how these layers contribute to the relationship among users, corporations, and publishers, I will find ways the Stack can be used to demonstrate how the components of a breach work such as the unbalanced hierarchy in the relationship of forms in a business model. For example, one of the sample models that I have worked on consists of five layers that compress a user's identity in a data structure. These five layers are the interface, social media, work information, home information, and personal information. In the model, each layer has laser-cut pieces that can be extracted using tweezers. This symbolizes the way corporations and unwanted third parties extract information out of users. They do not dump out information causing a mess. They subtly extract small bits of information so it is very difficult to tell their information is being mishandled until there is too much information lost.

While I am unsure how this environment will be utilized in this project, I want this project to be able to get a variety of reactions from users. It will start with a book that will describe the layers of the breach in a digestible way and present it to the public, hearing their opinions of the topic. After hearing their feedback and thoughts on the topic, the concept of connecting the Stack and the Breach will be reorganized into a small animation that will be easier to digest and understand based on the results. To encourage users to provide the desired reactions, the capstone needs to be engaging to the audience. The book will be visually interesting by being a layered book that can see through the variety of stack layers and see how they function. The animation is to show a different method to describe my research that will be digestible and easier to access on the internet.

What I wish for users to get out of this capstone project is that viewers will be able to understand the importance and awareness of how the breach can be fatal to users, especially those whose identities are composed of the internet. Most who use the internet frequently are slightly aware that their data can be used in undesirable ways, yet there isn’t a true call to action. This project should give doubts about the information they store on the internet or how it can be stored without content so they can tread the internet much more carefully.

Further Direction

There was a decent reception when I displayed my work outside of Pratt Institute. According to those who have attended, the primary feedback received was that the general message was unclear on what I was striving to achieve. My Thesis Capstone is meant to be a little vague on my position because I want my audience to think and develop their own opinions about the relationship among users, publishers, and corporations. Misinformation or bias is common when it comes to understanding how data is transferred on the internet. However, the format might have resulted in being a little too unclear on what I am talking about.

To finalize everything, I will make a more simple method to digest the message in my thesis capstone by creating a 1 minute animation discussing the Stack and how it relates to User Data and the breaches involved with it. It will be published on a site like Vimeo so it is easy to access. Overall, while the information was difficult to understand through the book, it was able to make my audience think about the topic which will linger in their minds. That is considered a success because this capstone isn't designed to make change, but meant to spread unbiased information to make the audience think for itself. As a result, the whole process from research to thesis capstone is considered a success.

Evaluation/Conclusion

According to Orberlo, there are approximately 4.33 billion users on the internet every day, which means there are 4.33 billion users with their own layers of privacy that are unaware of how their privacy is managed online. Of course, in the future, more people will become aware of how to protect themselves more efficiently when the internet gets older. It will be a matter of time when the issue of a data breach will be nullified, only for a new problem to resurface. It seems obvious to pin the blame on someone or something that users are experiencing these issues, which result in either corporations or publishers taking the blame. This is why corporations have this reputation of being greedy by taking everyone's information and using it to their advantage. There are examples where they are at fault such as Uber's failure to protect its users' data in 2016, but it isn't their fault all the time because the rise of technology leads to the rise of other openings for a data breach. Additionally, only the user is truly to blame because the user lacked the knowledge or didn't research enough on the consequences of his or her actions. Overall, this thesis is meant to encourage users to not pin the blame on the corporation for not cleaning up their mess, but to take initiative and research their own way to prevent their own data breach.

Bibliography

Easterling, Keller. Medium Design. Moscow: Strelka Press, January 12, 2018.
Easterling, Keller. Extrastatecraft. Brooklyn: Verso, August 16, 2016.

Hassenzhaul, Marc. “User Experience - A Research Agenda.” Taylor & Francis Online, Unknown Publisher, 4 March, 2011, https://www.tandfonline.com/doi/abs/10.1080/01449290500330331

Levine, Caroline. Forms, Rhythm, Hierarchy, Network. Princeton, New Jersey: Princeton University Press, 2015.

Noble, Safiya Umoja. Algorithms of Oppression: How Search Engines Reinforce Racism. New York University Press., 2018.

Peters, John, Durham. The Marvelous Clouds: Towards a Philosophy of Elemental Media. Princeton, Chicago and London: University of Chicago Press, 2015.

Foucault, Michael. Power/Knowledge: Selected Interviews and Other Writings. New York: Pantheon Books, 1980.

McLuhan, Marshall. Understanding Media. Cambridge, Massachusetts: MIT Press, 1994.

Agamben, Giorgio. What is an Apparatus? Stanford, California: Stanford University Press, 2009.

Danchev, Alex. 100 Artist Manifestos, Network. Princeton, London, United Kingdom: Penguin Classics, 2011.

Deleuze, Giles. What is a dispositif?. Unknown Location: Edited Books, 1992.

Hall, Sean. This Means This This Means That: A user’s guide to semiotics. London, UK: Laurence King Publishing, 2012.

Chan, Paul. “Paul Chan: ‘Our Data, Our Selves.’” e-Flux, 25 Sept. 2019, https://conversations.e-flux.com/t/paul-chan-our-da- ta-our-selves/9419.

Orjoux, Alanne. “YouTuber Etika Died by Suicide, Medical Examiner Says.” CNN, Cable News Network, 1 July 2019, www.cnn.com/2019/07/01/us/youtube-etika-desmond-amofah-suicide-trnd/index.html.

Clark, Josh. “How we hold our Gadgets.” A List Apart, Unknown Pub- lisher, 3 November, 2015, https://alistapart.com/arti- cle/how-we-hold-our-gadgets

The Stack
Mark Marino-Warren Sack - https://mitpress.mit.edu/books/stack

U.S. Dept. of Health and Human Services. The Research-Based Web Design & Usability Guidelines, Enlarged/Expanded edition. Washington: U.S. Government Printing Office, 2006. https://www.usability.gov/what-and-why/glossary/tag/interac- tion-design/index.html

Uber Paid Off Hackers To Hide a 57-million User Data Breach
Andy Greenberg -
https://www.wired.com/story/uber-paid-off-hackers-to-hide-a-57-million-user-data-breach/

Smuggling
https://www.ushistory.org/us/7d.asp

10 Internet Statistics every Marketer should know
Ying Lin - Oberlo
https://www.oberlo.com/blog/internet-statistics