Anonymity's Influence: Defining Anonymity as a Continuum to Proactively Design Online Environments to Combat Toxic User Behavior

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

Peter Morris

Spring, 2022

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor

Kathryn A. Neeley, Associate Professor of STS, Department of Engineering and Society

Introduction

In the United States, 93% of adults use the internet (NW et al., n.d.). According to the same poll, 99% of adults in the 18 to 29 age range use the internet. With the high levels of internet use, individuals find themselves in a tough position. Internet and web hosts leverage control over information and their users (Winkler & Zeadally, 2015, pg. 1). Research shows that hosts increasingly track web activities and store data on individuals in data mining efforts. Users don’t understand how much data is collected, what data is collected, nor the rules that govern the collection (Sardá et al., 2019). Once data has been collected, users have little control over how their data is used.

Given the high rate of internet use by American adults and the collection efforts of internet hosts, users may desire to protect their information by remaining anonymous. Anonymity provides a buffer between individuals and their data, but also introduces tradeoffs. Jordan observed that individuals will act differently depending on their perceived level of anonymity as it reflects the amount of personal responsibility associated with their actions (Jordan, 2019, pg. 5). Although anonymity can be used to protect users’ data, it also provides malicious actors the opportunity to harm online users. Currently, online environments are developed without considering the negative effects anonymity will have on human behavior. It is only after environments are implemented that designers react to those effects. This research reviews previous attempts to define anonymity, technological tools available to retain anonymity, and how anonymity affects behavior. I apply the discourse on design by Neeley and Luegenbiehl to determine criteria for toxic behavior which stems from anonymity. I lay out a path for online environment designers to evaluate potential threats from anonymous users and provide criteria to determine if their environment should include anonymous individuals.

Problem Definition: The State of Anonymity

As noted in the introduction, internet providers and technology companies have leverage over the information collected on users (Winkler & Zeadally, 2015, pg. 1). Browser history, online forms, and web searches are examples of online activities that providers track. The data is used for data mining and can be sold to third party vendors for targeted advertisements or improving website features. Users that want to reduce their online footprint should attempt to remain anonymous. Anonymity is difficult to retain because it is defined in many ways.

How to Define Anonymity:

In order to understand anonymity, I reviewed how previous authors defined anonymity. Winkler and Zeadally divides anonymity into three states: visual, disassociation, and lack of identifiability (Winkler & Zeadally, 2015, pg. 2). Visual anonymity is whether or not individuals can see each other while using the internet. Disassociation occurs when online users remove their name from communication; pseudonyms and usernames are common methods. Lack of identifiability is when an observer cannot distinguish between the activities of two users. Winkler and Zeadally offer one set of parameters to define anonymity. Eklund et al. argues that anonymity is a multi-layer phenomena affected by various actors (Eklund et al., 2021, pg. 2). Even if individuals attempt to conceal their identity, certain characteristics will emerge. Eklund et al. note that information can be inferred from how an individual types, talks, or moves in a game since social identity cannot be completely disconnected from their actions. Repeated interactions provide clues to users' identities. To better understand anonymity in different online environments over time, Eklund et al. reviewed online gaming (World of Warcraft) and online auctions (Tradera). Eklund et al. contrast online gaming with online auctions and propose three facets to define anonymity. The first facet is factual anonymity which links user information to a legal entity. For online gaming and auctions, users are factually known to the platform because of the legal structures required to access these platforms. Factual information known between users varies. For gaming, learning information is based upon the willingness of a user to share. For auctions, users are initially factually anonymous; however, the buyer and seller are identified after a successful bid. The second facet is social group anonymity which pertains to an individual's social identity. This information can be presented explicitly or known implicitly through repeated interactions. This presents itself as the feeling that individuals know each other. The final facet is physical anonymity which is information from embodied sources: visual, audio, and emotions. Visual information can include a picture or an avatar which ties the user to a real person. Eklund notes that it is harder to communicate online because the lack of body language and tone of voice.

The three facets proposed by Eklund et al. provide another lens to view anonymity. Similar to the states proposed by Winkler and Zeadally, the facets aren't mutually exclusive. Table 1 below compares the two sets of factors. Eklund et al. note that the facets exist within a framework which provide a reason to be anonymous online.

Anonymity State	Description	Example
Visual (Winkler)	Users have the opportunity to see each other	Web Camera
Disassociation (Winkler)	Users remove their name from interactions	Pseudonyms/usernames
Lack of Identifiability (Winkler)	Actions among multiple users cannot be attributed to its source	Forum where all users have the name "guest"
Factual (Eklund)	Information that links individual users to legal entities	Legal name, social security, credit cards, IP address
Social Group (Eklund)	Information that links a user to a larger group	The "I know you" feeling, group conformity
Physical (Eklund)	Information from embodied sources	Visual, voice, emotions, emoticons

Table 1: The table contrasts the different factors that cited authors use to quantify anonymity. Although the factors are different, both models are valid methods to describe anonymity.

Eklund presents the three facets within a framework of structures: legal, commercial, and technological. Legal structures result from government or platform regulations; they're usually an effort to protect personal identity. Commercial structures result from commercial interests of online actors. Examples include end user license agreements and terms of service contracts which specify what actions the user must take in order to gain access to the service. Users frequently accept such contracts without understanding or reading the agreements which gives leverage to the supplier. Technological structures include the hardware and software which facilitate online interaction. The three structures provide context for the three facets to exist in and their relationship is shown in Figure 1 below.

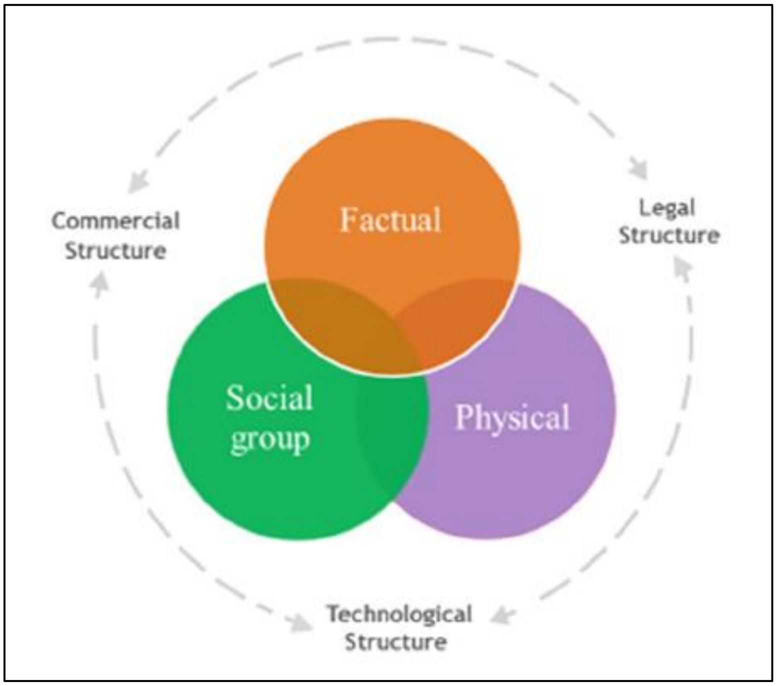

Figure 1 (adapted from Eklund et al., 2021, pg. 6): Visualization of Eklund et al proposed model for understanding anonymity. Online users are considered more anonymous when little information about themselves is known by other users. That information, as represented by the Venn diagram, can be separated into different, but overlapping, categories. Anonymity is bounded by a series of structures which make up the online environment and are represented by the dotted ring.

The model that Eklund et al. propose for determining anonymity is complementary to that described by Winkler & Zeadally. Both models split information into three categories. Although the categories overlap, they don't completely define one another. Therefore, anonymity shouldn't be dichotomous, neither completely known or unknown, since it is defined by several factors. The model proposed by Eklund et al. includes a structural framework which anonymity can exist in. Eklund et al. include a time component to consider how changes in information affect anonymity.

As individuals interact within the structures, information can be separated into categories which provide a convenient way to group information and indicates which information a user is more likely to share. However, sharing information in one category won't directly map into information in a different category. Therefore, anonymity is a continuum between known and unknown as shown in Figure 2 below. Defining anonymity on a spectrum reveals to the designers of systems that anonymity isn't static. Users have some control over their anonymity status by using tools.

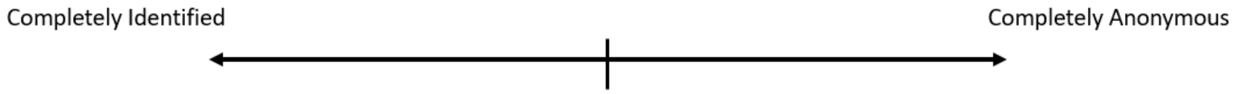

Figure 2 (created by author). Visualization of the continuum of anonymity. Information attributed to an online user does not completely reveal their identity. The amount information known about a user corresponds to a position on a continuum between two extremes: completely known and completely unknown.

How to Retain Anonymity:

There are several tools that online users can use to retain their anonymity. The most basic tool available is the incognito tab within internet browsers (Sardá et al., 2019, pg. 2). In the tab, virtual cookies are deleted upon browser exit. Cookies are unique identifies that are left in your browser by advertisers. Personal information is stored alongside cookie data in the cloud so companies can send personalized ads or search results. Incognito tabs don't stop administrators on the network from accessing their subordinate's searches.

Virtual private networks (VPNs) are another tool which change a user's IP address (Sardá et al., 2019, pg. 2). Each computer requires an IP address in order to connect to the internet (Winkler & Zeadally, 2015, pg. 3). Each address is unique, so it could be used to identify the user (Marx et al., 2018, pg. 3). When an VPN is active, the user's data is encrypted and sent through a secure tunnel. If an outside actor attempts to locate the user, the track will lead to the VPN's location rather than the user's location. Users should be aware that not all VPN services are free and companies who manage the services may use the user's data for marketing.

Another subset of tools are multilayer encryption networks which include Tor, JonDoNym, and I2P (Shahbar & Zincir-Heywood, 2018, pgs. 4-5). Tor (the onion router) provides layered encryption through three nodes. The user connects with an entry node in order to establish a data path. The information is relayed to an intermediate node and then the exit node which connects to web servers. As information is relayed, data layers are decrypted (like the layers of an onion) so that the data can find its next destination. This ensures the entire path of the data isn't known by a single node (Winkler & Zeadally, 2015, pg. 6). Nodes are run by volunteers who determine which type of traffic to allow through their nodes. I2P (Invisible Internet Project) is an extension to Tor. Multiple messages are tied together before being sent. Data is sent and received in unidirectional inbound and outbound tunnels. A network database controls the number of routers within the outbound tunnel, but doesn't allow users to see the tunnels. The tool was designed for private networks where both users were using I2P networks so the encryption is end-to-end. Communication with systems outside the I2P network may not have end-to-end encryption. JonDoNym performs a similar function. The user can pick two (free service) or three (paid service) mix servers to send their data through. The path through the mixes is fixed for a given session and is known as a cascade. When multiple different users access the services, all the connections are sent together to the first mix server. The data is sent through the remaining mix servers in accordance with transmission control protocol standards. The data from the final mixer is sent to an intermediary cache proxy through which the user can access their information requests. A downside to the multilayer encryption tools is it is difficult to communicate outside the network, so internet searches take more time. Each of the tools provides helps the individual retain different portions of their anonymity. However, the user must be cognizant of their behavior if the tools are to help.

Effects of Anonymity on Behavior:

The previous two subsections provide online designers information on how to define anonymity and how users achieve anonymity. This subsection reviews the effects anonymity has on users' behavior. Santana reviewed the speech of fourteen newspapers along the US-Mexico border to see how the comments of anonymous commenters differed from identified commenters. Dividing opinions of readers between uncivil, civil, and neither/nor, Santana found that 53% of anonymous comments were uncivil versus 29% of non-anonymous comments. Additionally, non-anonymous commenters were three times more likely to be civil. Santana concluded that the lack of social cues affected communication (Santana, 2014, pgs. 11-12). Newspapers in general ask readers to remain civil in their discourse. As newspapers transition online, an opening is created for anonymous users. Omernick and Sood examined the effects anonymity had on a social news site that transitioned from allowing anonymous comments to disallowing them (Omernick & Sood, 2013, pgs. 2-3). Comparing the comments, identified users' posts were more quantitatively more relevant and easier to read. Omernick and Sood used the Linguistic Inquiry and Word Count (LIWC) to assess the comments and found that unidentified users expressed more swear, anger, and negative emotion words. Deng performed a similar analysis on restaurant review platform that started to allow anonymous comments. Deng found that the overall rating of restaurants fell as more reviews expressed negative emotions (Deng et al., 2021, pgs. 7-8). A possible explanation for this behavior comes from research done by Lapidot-Lefler and Barak. In their research on interpersonal communication, anonymous individuals caused more threats, invisibility induced a negative atmosphere, and lack of eye contact led to higher self-reported flaming (Lapidot-Lefler & Barak, 2012, pg. 6). The research conducted by Santana, Omernick and Sood, Deng, and Lapidot-Lefler and Bark all show the negative effects that anonymity can have on online environments. Given the background research on anonymity, online designers need to pursue a purpose when creating environments.

Methods: Replacing Inevitability with Ethical Design

This section reviews the framework by Neeley and Luegenbiehl which contrasts a discourse on technological inevitability with a discourse on design. The initial paper presents its findings for a practicing engineer. However, the same logic should be transferable to a designer that is creating a system and who must consider tradeoffs associated with their system.

With respect to the two discourses discussed by Neeley and Luegenbiehl, the discourse on technological inevitability is more prevalent. The discourse perceives technology as an independent driver that follows a linear path of improvement. Increasing the efficiency of technology is the impetus for social change. Technological inevitability reduces the responsibility of an individual that contributes to a specific technology. Therefore, control over the outcome is impossible.

The discourse on inevitability paints the evolution of technology with broad strokes. It is a simplistic model that doesn't capture the nuances of a system. The means to share information could be seen using the discourse of inevitability. Initially, communication of information between individuals was face to face. Handwritten materials ensued which allowed individuals to pass information in a condensed form. Next followed the telegraph which enabled long distance communication. The radio allowed for the information to be spread by mouth to large number of individuals. The television built on the sound generated by the radios by adding pictures. Personal computer allowed individuals to communicate and get information that was relevant or desirable to them. Smart phones allowed individuals to leave their homes and still access information. The evolution of communication technology can be seen as efficiently transferring more information which aligns with the discourse of technological inevitability.

Neely and Luegenbiehl discuss the appeal of technological inevitability by referencing technological drift and technological momentum from Williams and Hughes respectively. Technological drift occurs when technological problems are quickly addressed to attain visible results. For the development of communication discussed above, information encoded by Morse code for the telegraph changed to information encoded in spoken language for the radio. The latter was easier for the masses to understand since it didn't require learning the encodings. Technological momentum states that once as technology incorporates a change, that change will affect future developments. Going back to the example, when communication changed from the radio to TV or TV to computers, using language to transfer information was reinforced. The thought experiment on the evolution of communication shows that the discourse of technological inevitability is appealing to apply. The simplicity of the design can be seen in Figure 3 below. The inevitability of technology (gravity) will cause technology (the ball) to progress. However, it breeds a lack of personal responsibility for effects that result from development which the discourse on design seeks to remedy.

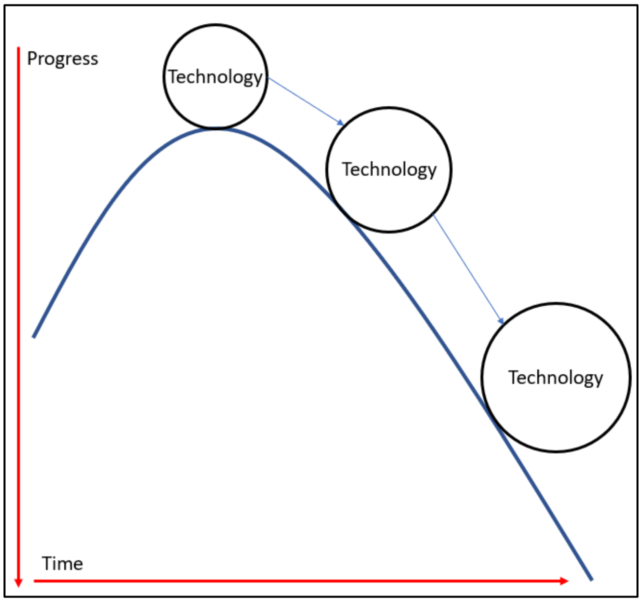

Figure 3: Discourse on Inevitability Model (Created by Author): The figure demonstrates the simplicity of the discourse on technological inevitability. As time goes by, technology progresses to become more efficient. The discourse doesn't take into account tradeoffs associated with the progress.

The discourse on design differs from the discourse on inevitability because it is centered around technological advancements made by individuals who design new products for a purpose. When an individual focuses on design, innovation becomes iterative since the designer is trying to achieve a specific goal rather than achieving the next logical step. Iteration endows designers with a sense of the tradeoffs necessary to complete a project as seen in Figure 4 below. A designer must be concerned with minute details of the project. Each problem that a design engineer encounters can never be perfectly captured. In order to understand the problem and implement a solution, relevant aspects are acted upon and irrelevant details are ignored. The problem a designer engages with must be simplified so that a practical solution can be implemented. Solutions are optimized to fulfill the greatest number of issues for a problem while recognizing that not all the needs will be met. Implementing one feature necessarily means excluding something else. There is not enough time, money, or resources to fulfill every requirement. Therefore, engineers and designers need to accept responsibility for the results that occur because of tradeoffs.

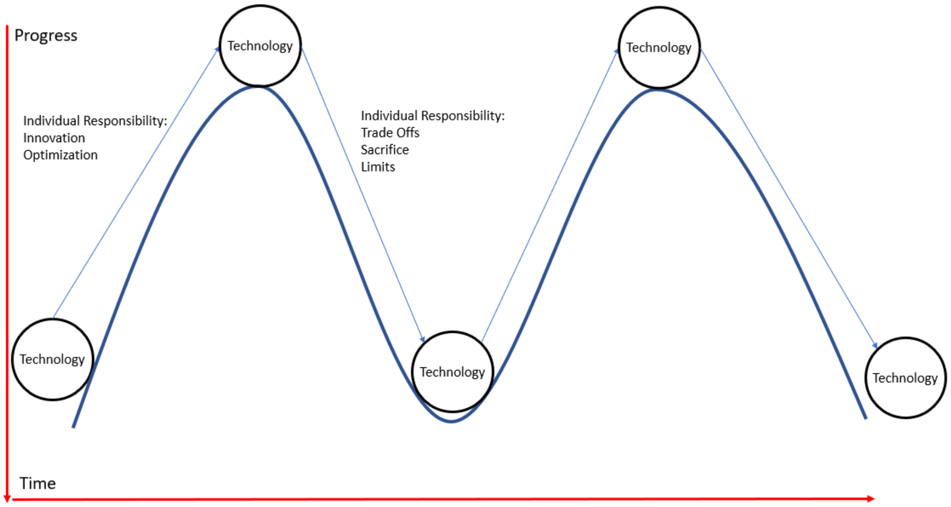

Figure 4: Discourse on Design Model (Created by Author): The figure demonstrates that as time goes by, technology is iterated by designers who have to make tradeoffs. Due to the sacrifices made in the design process, new technological products aren't on a linear path of improvement.

When a problem is first introduced, possible solutions are managed by commercial or political (social) actors. If a technical solution is required, engineers are introduced in order to design a feasible product. However, three questions posed by Neeley and Luegenbiehl affect the product: How does technology evolve? How are choices made to develop different technologies? Who makes these choices? With respect to the discourse of design, engineers design and adapt technologies to fit a solution determined by social actors in response to a problem. As engineers are the designers, it would be beneficial to include them in the solution process. An example from Rachel Carson's book *Silent Spring* provides a prudent example to why engineers should be involved in the process. In her book, Carson documents the negative impacts that pesticides, specifically dichlorodiphenyltrichloroethane (DDT), had on the environment. DDT was developed as an insecticide, but when it, DDT, was indiscriminately applied to the environment, it affected more than the intended pests. DDT adversely affected beneficial insects, fish, birds, and humans. Thus, Carson termed them biocides. The biocides which initially intended to help stop malaria caused more harm than good once pesticide resistance occurred and invasive species invaded a weakened ecosystem. This resulted because the chemical industry spread false information that was endorsed by public officials. Thus, there is a need for engineers, someone who retains responsibility for the results of their products, to look at the ethical implications. The ethics of a product need to be accounted for starting at the beginning, and continuing through the development. Iterations of the product and implementing a feedback loop will enable the engineer to strive for the greatest good through their implementation.

The discourse on technological inevitability is a simplistic answer that aligns products within an industry or for a company along an inevitable line of progress. All responsibility outside of the product functioning better is denied, undermining any ethical considerations. The discourse on design seeks to embolden engineers to take up the design process from the beginning by coming up with solutions in an effort to implement ethical products.

Results: Choosing Anonymous or Identified Environments

As noted in the background research, anonymity is not a binary state. Individuals are not fully known or unknown. An individual will be between the extremes based upon how cautious his is with his actions and how much information he divulges online. Given that anonymity is a sliding scale, designers need to understand what characteristics make up anonymity. Clark-Gordon separates anonymity between visual and discursive fields (Clark-Gordon et al., 2019, pg. 3). Visual anonymity is a user's physical representation and discursive anonymity is when a user's text cannot be attributed back to him. Eklund separates anonymity between physical, social group, and factual fields (Eklund et al., 2021, pgs. 9-13). Physical anonymity is the lack of information from an individual’s body and body language, social group anonymity is the broad characteristics that join individuals together, and factual anonymity is traceable information on an individual. Winkler and Zeadally separate anonymity between visual anonymity, disassociation, and lack of identifiability fields (Winkler & Zeadally, 2015, pg. 2). Visual anonymity is a user’s physical representation, disassociation is the lack of information tying an online user to a real person, and lack of identifiability is not being able to discern between individuals. Looking at a subset of the research material available, there are several ways to define anonymity which don’t completely agree. This is one of the reasons why it is hard to develop online systems that take into account the effects of anonymity.

Although the models use similar states for defining anonymity, the states are measured differs. Eklund’s groupings rely on a single individual while Winkler’s groupings rely on other individuals to engage with the “primary user”. Based on my research, I would define the facets of anonymity as intrapersonal and interpersonal. Anonymity just as reliant on an individual having a personal identity as it is reliant on other individuals which you can be compared to. Intrapersonal and interpersonal anonymity can be further broken down as shown in Figure 5 below. For intrapersonal anonymity, characteristic anonymity encompasses information that describes the user: examples include name, age, height, and sex. Behavioral anonymity encompasses information on the user’s action: examples include tone of voice, body language, and emotions/emoticons, type pattern. Visual anonymity includes the physical characteristics of a user: examples include eye color, hair length, and height. Similar to the facets by the researched authors, there is overlap between the subcategories. Visual information is personal and public, so it is subject to intrapersonal and interpersonal anonymity. The other subcategory under interpersonal anonymity is relative anonymity. Relative anonymity describes how information on members in a group is accumulated and interpreted. The facets of anonymity are a starting point on how system developers can understand their users and strategize how to implement different environments.

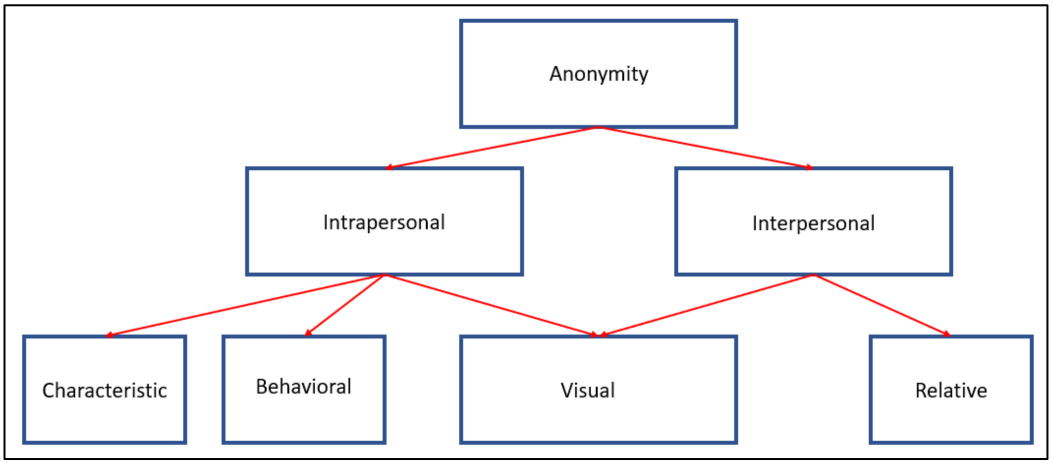

Figure 5: Defining Anonymity (Created by Author): This figure illustrates the author's attempt to define anonymity based upon the findings of other authors during research. The figure highlights the duality of anonymity which relies on the individual and outside actors.

Given my definition of anonymity, designers should use the definition to proactively address the effects anonymity could have on that environment. Currently, in order to access content, some environments require users to identify themselves while other it's optional. Newspaper comments, restaurant reviews, and online chatrooms are potential systems. As noted, systems are not designed with intention. Designers absentmindedly chose to allow or disallow anonymity and then react to the effects. From the background research, anonymous individuals are more likely to be affected by the disinhibition effect, and therefore are prone to posting material online that is toxic. A broad brush on opportunity can't justify removing anonymity over the entire internet. There are some online environments where anonymity has proven benign or beneficial to the users. By applying the framework from Neeley and Luegenbiehl, I note that designers of the online systems should be aware of the ethical implications that anonymity can have. Based on the kind of environment the designers wish to create, there should be an ethical discussion as to which anonymity environment is best. I start by examining what is the toxic behavior that anonymous individuals and how is it influencing or harming other users. From that point, I outline criteria that designers can refer to in order to take into account ethical implications of anonymous environments.

In order to determine what behavior should be considered toxic in an online environment, toxic behavior must be defined. Designers need to understand how the actions of one user negatively affect the online experience of another user. Toxic is defined as “containing or being poisonous material especially when capable of causing death or serious debilitation”. The term poisonous material is defined as “a substance that inhibits the activity of another substance or the course of a reaction or process”. From these two definitions, a reasonable definition for toxic behavior is the “actions performed by an individual or group of individuals that negatively affects the behavior or mindset of another individual or group of individuals”.

Using the definition for toxic behavior devised above, behaviors of online individuals need to be categorized to elicit trends of toxic activity so that criteria can be formed. The criteria are meant to inform designers of the effects of anonymity, but the criteria aren’t a solution. Two relevant behaviors to the effects of anonymity are lack of visibility and eye contact. Lack of visibility and eye contact on the internet lead to the disinhibition effect. This effect states that an individual is more likely to act rash because they are not trying to preserve their own social status nor conform to the societal standards. This behavior has the potential to be toxic, but is not toxic in of itself. A positive example is individuals that are more likely to share information about themselves without expecting anything in return. Two patients sharing advice on dealing with a specific disease might be easier than going to an in-person group. Advice isn’t limited to medical or personal affiliations. YouTube is a popular online site which has hundreds of thousands of hours of video tutorials. Either of these examples would not negatively bias other users to not return to the site. The other side of online disinhibition occurs when users act in a way to make other users not return. With respect to online textual exchanges in the comments sections of newspaper, individuals are more likely make rash decision in order to back up their stance and secure their position when emotions become involved. Online flaming, a grouping of hostile behaviors, includes aggressive language, swearing, derogatory names, negative comments, threats, and sexually inappropriate comments. The most severe action is a threat on someone else's life because it includes finding the targeted individuals and inflicting physical harm. The other side of the flaming behavior spectrum includes negative comments or swearing. While these actions are impolite, there is a distinction between impolite/unkind and uncivil.

Review sites that collect feedback on activities or places (restaurants, hotels, parks, etc.) have the potential to support negative behavior. Excluding the behavior of online trolls who aim to cause havoc, individuals using these review sites want to express their feelings on an experience. By providing anonymity, individuals are encouraged to present their true feelings without the fear. Social norms dictate that individuals generally post positive reviews. However, due to negativity bias in anonymous environments, individuals tend to hold any negative experience at a higher priority than the positive experiences. That environment will also cause any subsequent reviewer to exhibit more negative behavior if they notice that there are other negative comments on the platform. This again returns to the issue between impoliteness and incivility.

File sharing sites provide a different impetus for anonymity. For illegal file sharing, the individuals involved see that the public copyright laws are at odds current social values. Risking prosecution by the law is seen as less severe than getting the information for free. Anonymity supports these efforts by hiding IP addresses and user’s location from authorities looking to prosecute. This action is impolite, but is also is uncivil as the transgressor is denying the content creator’s right to receive compensation for his work.

Based upon the different scenarios provided, designers of systems need to take into account the potential for impoliteness, incivility, and illegality. Each of the three behaviors should be weighted differently because what the behaviors entails are substantially different. The environment chosen should reflect the amount of responsibility that needs to be taken by the users. Additionally, designers need to consider what the human-to-human interaction is going to be. A person-to-person interaction is different from a person to an entity or person to internet. Environments that have interactions between fewer users should be scrutinized more because the experience between individuals is more personal. However, it is the responsibility of the designers to balance the options in order to ethically implement online systems which aspire to fulfill their function while minimizing negative consequences.

Factors for Designers	
Feature	Concerns
Environment	Number of People Type of content
Interactions	Person-to-person Person-to-entity
Consequences	Impolite Uncivil Illegal

Table 2: Factors for Designers (created by author). This table reviews features of online systems that the designers need to be aware of to proactively account for the effects of anonymity.

Conclusion:

Interactions on the internet are facilitated by many sites and environments that users can access. Anonymity is a difficult issue to define as illustrated through the research by Winkler and Zeadally, Eklund et al, and Clark-Gordon. The issues that define anonymity have influenced the way that designers of online systems evaluate whether or not to allow anonymity in their environment. Previously, designers arbitrarily chose whether individuals could be anonymous and then reacted to the consequences of including anonymity. As shown through Deng's research, identified individuals used "less swear words, less angry words, more affect words, more positive emotion words, and less negative emotion words" (Deng, 2021, pg. 5).

Therefore, online designers need to proactively evaluate the potential effects anonymity could have on their systems. Using the discourse of design by Neeley and Luegenbiehl, I showed designers have a responsibility to manage tradeoffs associated with implementing their product. Therefore, I developed criteria which attempt to model what a beneficial analysis could look like. However, throughout this paper, I assumed that each environment implemented by a designer will respond to anonymity the same way. Grouping all the environments in my analysis allowed me to pull out trends I thought were useful. Thus, the criteria I developed are broad in nature. Nevertheless, the criteria I developed are useful because the criteria proactively engage with system designers. System designers have the opportunity to purposefully design their product to balance the implications of anonymity with the function of their environment.

References

Clark-Gordon, C. V., Bowman, N. D., Goodboy, A. K., & Wright, A. (2019). Anonymity and Online Self-Disclosure: A Meta-Analysis. *Communication Reports, 32*(2), 98–111. https://doi.org/10.1080/08934215.2019.1607516

Deng, L., Sun, W., Xu, D., & Ye, Q. (2021). Impact of Anonymity on Consumers' Online Reviews. *Psychology & Marketing, 38*(12), 2259–2270. https://doi.org/10.1002/mar.21565

Eklund, L., von Essen, E., Jonsson, F., & Johansson, M. (2021). Beyond a Dichotomous Understanding of Online Anonymity: Bridging the Macro and Micro Level. *Sociological Research Online*, 13607804211019760. https://doi.org/10.1177/13607804211019760

Jordan, T. (2019). Does online anonymity undermine the sense of personal responsibility? *Media, Culture & Society, 41*(4), 572–577. https://doi.org/10.1177/0163443719842073

Lapidot-Lefler, N., & Barak, A. (2012). Effects of anonymity, invisibility, and lack of eye-contact on toxic online disinhibition. *Computers in Human Behavior, 28*(2), 434–443. https://doi.org/10.1016/j.chb.2011.10.014

Marx, M., Sy, E., Burkert, C., & Federrath, H. (2018). Anonymity Online – Current Solutions and Challenges. In M. Hansen, E. Kosta, I. Nai-Fovino, & S. Fischer-Hübner (Eds.), *Privacy and Identity Management. The Smart Revolution: 12th IFIP WG 9.2, 9.5, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School, Ispra, Italy, September 4-8, 2017, Revised Selected Papers* (pp. 38–55). Springer International Publishing. https://doi.org/10.1007/978-3-319-92925-5_4

NW, 1615 L. St, Washington, S. 800, & Inquiries, D. 20036 U.-419-4300 | M.-857-8562 | F.-419-4372 | M. (n.d.). Demographics of Internet and Home Broadband Usage in the United States. *Pew Research Center: Internet, Science & Tech*. Retrieved February 21, 2022, from https://www.pewresearch.org/internet/fact-sheet/internet-broadband/

Omernick, E., & Sood, S. O. (2013). The Impact of Anonymity in Online Communities. *2013 International Conference on Social Computing*, 526–535. https://doi.org/10.1109/SocialCom.2013.80

Santana, A. D. (2014). Virtuous or Vitriolic. *Journalism Practice*, *8*(1), 18–33. https://doi.org/10.1080/17512786.2013.813194

Sardá, T., Natale, S., Sotirakopoulos, N., & Monaghan, M. (2019). Understanding online anonymity. *Media, Culture & Society*, *41*(4), 557–564. https://doi.org/10.1177/0163443719842074

Shahbar, K., & Zincir-Heywood, A. N. (2018). Weighted Factors for Evaluating Anonymity. In A. Imine, J. M. Fernandez, J.-Y. Marion, L. Logrippo, & J. Garcia-Alfaro (Eds.), *Foundations and Practice of Security* (pp. 303–318). Springer International Publishing. https://doi.org/10.1007/978-3-319-75650-9_20

Winkler, S., & Zeadally, S. (2015). An analysis of tools for online anonymity. *International Journal of Pervasive Computing and Communications*, *11*(4), 436–453. https://doi.org/10.1108/IJPCC-08-2015-0030