Privacy and the Struggle to Preserve it: Reevaluating Big Tech through Contemporary Literature

PRIVACY AND THE STRUGGLE TO PRESERVE IT:
REEVALUATING BIG TECH THROUGH CONTEMPORARY LITERATURE

by

Veronica Tang

A thesis submitted to the
Departments of Computer Science
and English in partial fulfillment of
the requirements for a joint
Bachelor's Degree

March 7, 2022

Contents

Introduction

As Stephanie LeMenager writes, "The humanities are fundamentally a project of shoring up cultural memory and rendering it usable for what cannot be predicted but, in some shape, may have happened before."[1] The widespread use of digital technology and the problems that accompany it are relatively new, but the concept of privacy existed long before the advent of modern technology. The boundaries that traditionally defined it have merely shifted, and the flow of information between individuals and institutions has drastically changed as a result. Contemporary literature, as a repository of cultural memory and a reflection of cultural attitudes surrounding technology and privacy, provides valuable insight into the impact of these shifting boundaries. Furthermore, by defamiliarizing the challenges presented by modern technology, I argue that contemporary fiction reveals the ethical and practical issues at stake. Therefore, this thesis aims to redefine digital privacy as a form of authorship and to illuminate struggles to preserve it by examining data and surveillance through the lens of contemporary literature. It also aims to define a new genre that I call the tech gothic, which is comprised of 21st-century novels that convey fear and terror of new technology by drawing on motifs of traditional gothic literature, translated to fit within the new landscape of Big Tech and the digital age.

The three novels examined in this thesis — *New Waves* (2020) by Kevin Nguyen, *Little Brother* (2008) by Cory Doctorow, and *The Circle* (2013) by Dave Eggers — engage with privacy crises in the tech industry and issues of government surveillance. Although these novels span young adult fiction, dystopian writing, workplace dramas, and bildungsromans, they all are

[1] Stephanie LeMenager, "Climate Change and the Struggle for Genre," in *Anthropocene Reading: Literary History in Geologic Times* (University Park, PA: The Pennsylvania State University Press, 2017), pp. 220-238, 236.

shaped by fundamental privacy tradeoffs in technology. *New Waves* is a novel about a young man named Lucas, who works at a startup, Phantom, which is a platform for sending messages that are quickly deleted. During the course of the novel, he deals with the death of his close friend and co-worker, Margo. Through the digital footprint that Margo left while she was alive, Lucas discovers completely new aspects of her identity. Meanwhile, *Little Brother* tells the story of Marcus, a high school student living in a heavily surveilled, near-future San Francisco. Marcus creates his own private mesh network as a form of resistance after being detained by the Department of Homeland Security in the wake of a terrorist attack, and he eventually succeeds in bringing about an end to the inhumane interrogation and surveillance tactics that police have been using in an attempt to root out terrorists. And finally, *The Circle* is set in a hypothetical future in which a major tech company called the Circle has come to control all aspects of life. Their primary product is TruYou, which allows users to aggregate all their online needs on a single platform. They make a wide variety of other products as well, like trackers that can be embedded in children's bones to keep them safe from kidnappers, cameras that livestream surveillance video in high quality at all times, and deep-sea submarines for exploring the Mariana Trench. The protagonist of *The Circle* is Mae, a new employee at the Circle who initially begins in customer service but rises quickly through the company's ranks by creating and promoting the axioms "Secrets are lies," "Sharing is caring," and "Privacy is theft."

I read these novels alongside current privacy legislation (such as the EU's General Data Protection Regulation, the California Consumer Privacy Act, the Health Insurance Portability and Accountability Act, and the Family Educational Rights and Privacy Act), Supreme Court case records (*United States v. Jones* and *United States v. Maynard*), and articles about events in tech history that exemplify fundamental privacy tradeoffs. These sources help to establish the

current state of privacy legislation and draw real life parallels to the scenarios explored in *New Waves* and *Little Brother*. I also engage with nonfiction books that have notably shaped discourse on the role of privacy and technology in society: Shoshana Zuboff's *The Age of Surveillance Capitalism,* Safiya Umoja Noble's *Algorithms of Oppression,* and Helen Nissenbaum's *Privacy in Context*. These texts provide valuable insight into the privacy practices of Big Tech, as well as a framework for understanding changes to traditional flows of information that negatively impact consumers. My analysis uses theoretical conceptions of privacy, such as Dan Geer's assertion that privacy constitutes "the power to selectively reveal oneself to the world," as well as technical ideas from computer science, such as differential privacy.

My argument unfolds in two steps. In my first chapter, I develop a new framework with which to understand data privacy by drawing on literary theories of authorship. "What is an Author?" by Michel Foucault and "The Death of the Author" by Roland Barthes serve as the theoretical foundations for understanding privacy from the perspectives of the user and third parties, respectively. The repositories of an individual's online data fulfill properties that Foucault ascribes to literary works that produce an "author function," and so, I argue, can be usefully interpreted as a "work" that the user has authored. Just as there is a difference between an author's biographical self and the "second self" that they present through their literary work, consumers should have the ability to shape representations of themselves that they put forward in their "work" of digital data. Likewise, from a third party's perspective, complete privacy means that the author, or rather, user, is fully indistinguishable from nothing (which corresponds to (0,0)-differential privacy). In other words, the physical author should not exist to the third party in any form other than the one that they have chosen to represent themselves as online.

In my second chapter, I analyze privacy tradeoffs exposed by past incidents (like the FBI-Apple encryption dispute and Yik Yak's harassment scandal) and theorize a new genre, the "tech gothic," which adapts the characteristics of the traditional gothic novel to the new landscape of Big Tech. I argue that *New Waves, Little Brother,* and *The Circle* can all be classified as works of tech gothic and that they reflect the social anxieties and fears within contemporary society that have resulted from the shift in traditional boundaries of privacy instigated by technology. Their hyperbolic plots and scenarios, though unlikely to occur in the near future, correspond to the edge cases used in computer science to test the comprehensiveness of algorithms, and therefore embody many ethical and practical challenges to implementing data privacy. These novels and events demonstrate that there are necessary privacy tradeoffs that society has yet to resolve, revealing that the current place at which the new boundaries of privacy exist in reality is distinct from the place they should be drawn. A universal consensus on what an appropriate threshold looks like has yet to be reached, but Helen Nissenbaum's framework of contextual integrity provides a starting point for establishing this threshold.

Ultimately, the goals of this thesis are to cast new light on debates surrounding technology and privacy, to reexamine the definition of privacy and how it should be implemented through the lens of contemporary literature, and to demonstrate the value of humanistic knowledge in questions of privacy. I render authorship and genre usable in an age of increased technological power; these stories, as repositories of cultural memory, will be critical in establishing the social norms that form the foundation of the compromises technology must make.

Chapter 1: Privacy as Authorship

In Kevin Nguyen's debut 2020 novel, *New Waves*, the protagonist, Lucas, tells a story about a time that he and his friend Margo attempt to learn about an obscure Japanese musician. It takes them "a colossal effort to dig up anything about this artist."[2] They never learn anything about him beyond the motivation for his music and the city that he lived in, and they describe him as a "recluse." This scene raises questions about the limits of online privacy: to what extent can a person separate themselves from the material they produce and share online? Is anonymity of the composer sufficient, or does true privacy require more? How crucial is it for users to control the way they represent themselves online? In this chapter, I argue that privacy is a form of authorship, such that the "work" that users produce as authors are their online repositories of personal data.

Definitions of Privacy

Privacy is an issue that technology companies too often ignore, a concern that politicians attempt to regulate, a black box that confuses most consumers, and a concept that computer scientists attempt to theorize in statistical terms. For most people who use the internet, privacy is a genuine concern, since completing nearly any action online reveals details about one's preferences or personal information to third parties. And with the increasing number of internet users today as well as the increased pressure on consumers and workers alike to use technology to complete everyday tasks, traditional boundaries that defined personal privacy in the past have shifted. As Shoshana Zuboff writes in *The Age of Surveillance Capitalism,* "all aspects of human

[2] Kevin Nguyen, *New Waves: A Novel* (Random House Publishing Group, 2020), 126.

experience are claimed as raw-material supplies and targeted for rendering into behavioral data" by corporations, and tech companies use consumers' appetite for greater convenience and enhanced personalization as "camouflage for aggressive extraction operations that mine the intimate depths of everyday life."[3] Many people take their cellphones with them when they leave their home in the mornings, log on to a computer during their time at work, stop to scroll through social media during a break, pass by security cameras as they make their way from place to place, and return home for an evening of video games or Netflix. In the process, they reveal information about their location, habits, preferences, and routines to the providers of the many services that they use throughout the day. This lifestyle pervades wealthy countries, such that most of us are never far from a device that collects and analyzes our data or siphons it off to another entity.

More people have become aware of the struggle to preserve personal privacy online in recent years; in the United States, at least, privacy features in news headlines along with the names of Silicon Valley superpowers from time to time, and it shows up on propositions in California periodically. California Proposition 24, for example, was recently enshrined as the California Privacy Rights Act of 2020, which established the California Privacy Protection Agency in order to "further protect… the constitutional right to privacy."[4] However, privacy exists in the cultural consciousness as a rather amorphous concept; consumers, engineers, and lawmakers each have their own ways of understanding privacy, and each method has varying

[3] Shoshana Zuboff, *The Age of Surveillance Capitalism: the Fight for a Human Future at the New Frontier of Power*, (PublicAffairs, 2019), 19.
[4] "California Proposition 24, Consumer Personal Information Law and Agency Initiative (2020)," Ballotpedia, https://ballotpedia.org/California_Proposition_24,_Consumer_Personal_Information_Law_and_Agency_Initiative_(2020).

degrees of imprecision and applicability. For instance, most consumers relate to privacy affectively: the perceived invasion of their privacy causes a vague feeling of discomfort or a nagging suspicion that the current situation, in which something or someone has more of their data than they had originally bargained for, is unsettling. There is a complete lack of understanding about privacy among the general public: while 79% of adults in the United States are concerned about how companies are using their personal data, only 6% of adults claim to actually understand what companies do with it.[5] And so, though the discomfort and concern that most consumers feel are entirely valid responses to the practices that many technology companies engage in today, their feelings about privacy are generally very vague and do not concretely define that which has been infringed upon.

Computer scientists, on the other hand, tend to think of privacy in terms of data management practices, particularly how long specific data is retained and which parties have access to it. They have also formally defined several methods of anonymization, like k-anonymity, l-diversity, and differential privacy. Differential privacy, in particular, has been growing in popularity within the field in recent years, and it was the privacy-preserving mechanism used in the United States 2020 Census. Differential privacy is a property that is satisfied when the algorithm or process in question returns indistinguishable outputs when run on two databases that differ by only one individual.[6] In the words of Cynthia Dwork and Aaron Roth, differential privacy is a "promise made by a data holder… to a data subject: 'You will not

[5] Brooke Auxier et al., "Americans and Privacy: Concerned, Confused and Feeling Lack of Control over Their Personal Information," Pew Research Center: Internet, Science & Tech (Pew Research Center, August 17, 2020), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.
[6] Damien Desfontaines, "Why Differential Privacy Is Awesome," Ted is writing things, July 30, 2018, https://desfontain.es/privacy/differential-privacy-awesomeness.html.

be affected, adversely or otherwise, by allowing your data to be used in any study or analysis, no matter what other studies, data sets, or information sources are available.'"[7] This promise is upheld by the mathematical definition of differential privacy, which ensures that the certainty of all information that a potential adversary attempts to infer will be bounded by a specified range of probabilities. In this way, a differentially private mechanism reveals no previously unknown information about any given person in the database to an attacker. These practices imply that, for computer scientists, privacy can be measured by the difficulty of re-identifying or learning more about an individual in a dataset and by the difficulty for unauthorized parties to access encrypted data. But while limited data retention, encryption, and differential privacy are undoubtedly all useful tools for preserving and quantifying privacy, they really only apply to *data* privacy. Privacy can be violated in cases where data is not being collected or analyzed; for example, someone could plant a camera in your room and watch you constantly. Even if they do not record or analyze your actions, they would still be invading your privacy. Therefore, these conceptions of data privacy are not universal enough to constitute a definition of privacy as a whole.

And while privacy exists as a legal concept, its definition varies from country to country and state to state. The United States legal system guarantees a "reasonable expectation of privacy" — a somewhat vague notion that "someone who unreasonably and seriously compromises another's interest in keeping her affairs from being known can be held liable for that exposure or intrusion."[8] Based in the Fourth Amendment, the "reasonable expectation of

[7] Cynthia Dwork and Aaron Roth, *The Algorithmic Foundations of Differential Privacy* (Hanover: now Publishers Inc, 2014), 5.
[8] "What Is the 'Reasonable Expectation of Privacy'?," Findlaw, July 17, 2017, https://www.findlaw.com/injury/torts-and-personal-injuries/what-is-the--reasonable-expectation-of-privacy--.html.

privacy" prevents "unreasonable searches and seizures."[9] It has developed piecemeal through Supreme Court rulings over the years, and the line drawn by reasonable expectation of privacy is blurry at best. For instance, in the 2012 case, *United States v. Jones*, the Court ruled that the GPS tracking used to surveil Antoine Jones constituted a "search" and violated his Fourth Amendment rights — but the length of the surveillance played an important part in the ruling. Jones was monitored for twenty-eight days, and Justice Ginsburg specifically stated that these twenty-eight days "considered as a collective whole" were sufficiently invasive to constitute an unreasonable violation of privacy.[10] However, one cannot help but wonder what the decision would have been if the duration of the tracking period had been shorter. When does permissible surveillance become a violation of privacy? After twenty days? Fifteen? Ten? When does such surveillance require the oversight of a judge? Evidently, "reasonable expectation of privacy" can hardly be considered a concrete definition.

On the other hand, the California Consumer Privacy Act (CCPA), while not comprehensive by any means, offers more concrete criteria than the doctrine of reasonable expectation of privacy and specifically concerns data collection by corporations. CCPA stipulates new privacy rights for California consumers, including the right to be informed, the right to delete personal information, the right to opt-out of its sale, and the right to nondiscrimination for exercising their CCPA rights.[11] The European Union has its own legal framework for data privacy, the General Data Protection Regulation (GDPR). Though it was the model that inspired many other privacy laws across the world, including CCPA, GDPR differs

[9] U.S. Const. amend. IV.
[10] Orin S. Kerr, "The Mosaic Theory of the Fourth Amendment," 111 MICH. L. REV. 311 (2012), 324.
[11] "California Consumer Privacy Act (CCPA)," State of California - Department of Justice - Office of the Attorney General, January 27, 2022, https://oag.ca.gov/privacy/ccpa.

from CCPA in that it is more expansive. GDPR enumerates the following basic privacy rights: the right to be informed, the right of access, the right to rectification, the right to erasure, the right to restrict processing, the right to data portability, the right to object, and rights in relation to automated decision making and profiling.[12] GDPR and CCPA both share a common ancestor in the United States Federal Trade Commission's fair information practice principles. These principles resulted from the Commission's 1998 investigation on online privacy issues, which identifies "five core principles of privacy protection: (1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and (5) Enforcement/Redress."[13]

Despite the similarities between GDPR and CCPA, there are still fundamental differences that set the two apart. CCPA focuses primarily on the company that is holding a user's information, while GDPR centers on the individual whose data is being collected. This shift in focus has significant repercussions; for instance, the right to erasure detailed by GDPR, also known as the right to forget, is stronger than the right to delete personal information in CCPA as a result. The right to erasure allows people to delete "erroneous, false, or downright private information"[14] in Google search results — which, despite the name, functions more like the right to be *unindexed* instead of completely deleted — whereas the right to delete personal information only covers personal information that businesses have themselves gleaned from consumers. As Safiya Umoja Noble notes in *Algorithms of Oppression*, the right to forget is particularly important given that search results have become the newest "battleground over the identity,

[12] "What Is GDPR, the EU's New Data Protection Law?," GDPR.eu, February 13, 2019, https://gdpr.eu/what-is-gdpr/.
[13] *Privacy Online: A Report to Congress* (WASHINGTON, D.C.: THE COMMISSION, 1998), 7.
[14] Safiya Umoja Noble. *Algorithms of Oppression*. (New York: NYU Press, 2018), 122.

control, and boundaries of legitimate knowledge."[15] Google's popularity has led it to be perceived as, in some ways, the "official record" of the self; it is what the rest of the world knows about any given individual and how the world will choose to validate information about that person.[16] The right to forget is limited, since one must demonstrate that the information in question is no longer relevant. But given how crucial a person's search results are as a representation of their identity to the rest of the world, the restricted control over search results provided by the right to forget is still a notable improvement over CCPA's right to delete personal information.

Some countries, in contrast, offer no legal right to privacy. For example, in 2019, China enforced a series of regulations to curb video gaming, including a cyber-curfew banning those under 18 from playing video games between 10 pm and 8 am. To help enforce these regulations, Tencent Games is now using facial recognition to verify the ages of players during curfew hours, so that underage users cannot use other devices that they do not own to login and play videogames.[17] Users who fail or reject the facial recognition mechanism are refused access to their accounts. This facial recognition mechanism, while effective at enforcing China's cyber-curfew, also means that anyone attempting to *play a video game* after 10 pm will have their image data recorded and analyzed by an algorithm that will then classify them as above or below 18 years old. This system implements highly invasive surveillance for the sake of curbing adolescent gaming; as an example of its impact, there was even a trending hashtag on Weibo, a

[15] Noble, *Algorithms of Oppression,* 122-123.
[16] Ibid, 122.
[17] Tiffany May and Amy Chang Chien, "Game over: Chinese Company Deploys Facial Recognition to Limit Youths' Play," The New York Times (The New York Times, July 8, 2021), https://www.nytimes.com/2021/07/08/business/video-game-facial-recognition-tencent.html.

microblogging platform, reminding Chinese netizens to wear proper clothing while gaming in case their cameras captured pictures of more than just their faces. In some places, there *is* no legal definition of privacy, and personal privacy can be violated on a large scale for relatively trivial reasons.

Privacy as Authorship

Clearly, there are many vague, incomplete, and inconsistent definitions of privacy that different entities have developed over time. Dan Geer, however, insightfully identifies the operational core of digital privacy as "the power to selectively reveal oneself to the world," or rather, "the effective capacity to misrepresent yourself."[18] He justifies this definition by stating that, "in choosing what to reveal, however idiosyncratically, we demonstrate our liberty."[19] Following Geer's reasoning, I argue that we can understand privacy as a form of authorship. In going about our daily lives, we produce a "work," in the form of the repository of our digital data — social media posts, photos stored in the cloud, shopping histories on online websites, search engine histories, and messages sent to others — and privacy would give us agency over this work. We would have control over this repository of our digital data, and we would be able to manipulate it as we see fit so that we may represent ourselves in the ways that we choose.

In his essay, "What is an Author?", Foucault theorizes the role of the author and suggests that a text that produces the "author function" generates a projection of an individual creator with certain attributes. Not all works construct an "author" in this way, and Foucault identifies four characteristics of texts that produce the "author function" — all of which can be applied to the

[18] Dan Geer, "The Right to be Unobserved" in *IEEE Security & Privacy* (New York, NY: IEEE Computer Society, 2015) pp. 88, 88.
[19] Ibid.

repositories of online personal data that we produce as users and consumers. Firstly, Foucault states that books or texts with authors are "objects of appropriation."[20] These books or texts are *property* of their authors in "the legal and institutional systems that circumscribe, determine, and articulate the realm of discourses,"[21] through our society's system of ownership, copyright, and intellectual property. Similarly, in an ideal world where online privacy is respected and enforced, digital data would be the legal property of the user as well.

Secondly, the author-function is "not universal or constant in all discourse."[22] In other words, the nature of authorship varies depending on the type of text that the author has produced. Foucault provides examples of how different type of texts may or may not have required attribution to specific authors for the sake of validation and how this dynamic has changed over time. In the Middle Ages, "literary" texts like stories, folk tales, and epics were widely accepted as authentic due to their supposed age, while "scientific" texts that dealt with medicine, the natural sciences, or geography required the name of an established author (such as Hippocrates or Pliny) in order to be considered truthful. This dynamic shifted in the seventeenth and eighteenth centuries, however, when scientific texts became "accepted on their own merits and positioned within an anonymous and coherent conceptual system of established truths and methods of verification,"[23] whereas literary texts began to require an author's name to be accepted. And so, much as the ownership and attribution of traditional written works vary depending on the circumstances and context, so does the ownership and attribution of data to individuals. In the United States, for example, there are specific laws concerning health and

[20] Michel Foucault, "What is an Author?" in *The Foucault Reader* (New York: Pantheon Books, 1984), 108.
[21] Ibid, 113.
[22] Ibid, 109.
[23] Ibid.

education data, known as the Health Insurance Portability and Accountability Act (HIPAA) and the Family Educational Rights and Privacy Act (FERPA), respectively. HIPAA and FERPA set aside health information and student education records as unique classes of personal information that must be treated differently from other types of data. HIPAA regulates the uses and disclosures of patient health information, allowing it to only be disclosed after being properly anonymized or only under a list of specific circumstances.[24] FERPA, on the other hand, "gives parents or eligible students more control of their educational records" and requires that educational institutions obtain written consent before disclosing "personally identifiable information in education records."[25] And while FERPA also allows for the sharing of de-identified information, its definition of "de-identified" is actually different from that of HIPAA. Therefore, just as the ownership and attribution of literary texts to individuals varies, the ownership and attribution of data is oftentimes also regulated differently depending on the context.

Furthermore, Foucault states that the author-function is "not formed spontaneously through the simple attribution of a discourse to an individual."[26] He points out that there is a tradition dating back to Christian exegesis of deducing which texts belong to a given author by looking for a certain set of consistencies between texts. Therefore, the author-function includes a specific set of criteria that can be used to determine whether the stated author actually did write the work. These criteria have changed over time — as Foucault notes, the strategies adopted by

[24] "Health Insurance Portability and Accountability Act of 1996 (HIPAA)," Centers for Disease Control and Prevention (Centers for Disease Control and Prevention, September 14, 2018), https://www.cdc.gov/phlp/publications/topic/hipaa.html#one.
[25] "Health Information & Privacy," Centers for Disease Control and Prevention (Centers for Disease Control and Prevention, September 14, 2018), https://www.cdc.gov/phlp/publications/topic/healthinformationprivacy.html.
[26] Foucault, "What is an Author?", 110.

modern criticism differs from those of Christian exegesis to some extent — but they exist all the same. Likewise, there are standard practices used to authenticate users that determine whether or not someone actually owns an online account. Kevin Nguyen sums it up quite succinctly in *New Waves*: oftentimes, logging in to a device or website involves two-factor authentication, which relies on "something you know and something you have"[27] to confirm your identity. This "something you know" is typically a password, though it can include security questions that were designated at the time the account was created, whereas the "something you have" is usually a physical device (like a phone or fob).

Finally, Foucault states that the author-function "does not refer… to an actual individual insofar as it simultaneously gives rise to a variety of egos and to a series of subjective positions that individuals of any class may come to occupy."[28] The narrator of a text is naturally not identical to the author, and the voice that the author adopts in their work does not exactly reflect who they are in reality. Instead, there is what Foucault calls a "second self whose similarity to the author is never fixed and undergoes considerable alteration within the course of a single book."[29] This division between the author's original self and second self is a crucial element of the author-function, and it exists for individuals with online profiles as well. It is most easily illustrated by example; the following screenshot is taken from data that my friend, Tim, requested from Amazon as required by the EU's General Data Protection Regulation (GDPR):

[27] Nguyen, *New Waves*, 55.
[28] Foucault, "What is an Author?", 113.
[29] Ibid, 112.

A	B	C	D	E
Audiences in which you are included via 3rd Parties				
Automotive:Investible Assets - (between $50k and $99k)				
Automotive:Not In Market For - Auto:Used 6+ years old				
Demographics:Age Range:25-34				
Demographics:Education:Graduate degree				
Demographics:Home Owners				
Demographics:Income:50k - 75k				
Demographics:Length of residency:11 or more years				
Demographics:Male				
Demographics:No Children in Household				
Demographics:Number of adults in household:3 adults				
Demographics:Occupation:Sales/Service				
Demographics:Property value:$400k+				
Demographics:Unmarried				

This information on Tim is accurate on some accounts, for he is indeed male and unmarried. But the rest of it is wildly inaccurate, which demonstrates that there is indeed a separation of a user's original self and the identity that they operate under online — while Tim is a 22-year-old undergraduate student, he apparently shops like a 30-year-old salesperson with a graduate degree, who has lived in one place for 11 or more years. This is one of his many alter egos; though he does not have complete control in its construction, it is indeed a "second self" that is distinct from his original self, created by his actions on the Amazon website in conjunction with an algorithm that analyzes and classifies the nature of these actions. This trove of data is also subject to Foucault's three other criteria: we are allowed to request it because of the legal regulations, the details and accessibility of the data vary depending on the context (advertising, addresses, device information, Alexa, etc.), and in order to access this data, there is something we must know (a password), as well as something we must own (access to the email account through which the Amazon account was created). And so, we can see that the author-

function that Foucault describes is fulfilled by most users of online services, such that the work they produce is their repository of digital data.

This framework of internet users as authors gives us a way to define privacy: for users, true privacy is the ability to dictate the "second self" that Foucault describes. Users must have the agency to choose exactly how they present their "work" (their digital record) to the rest of the world — tech companies, governments, and other users alike. Unlike Tim, whose representation as a 30-year-old salesman was determined by Amazon's classification algorithms and not his own free will, users with complete privacy would be able to choose their own alternate identities. The entire archive of their online material — including that which is unearthed by the search engine results that have come to function as the world's record of legitimate knowledge — would be subject to their explicit control.

Privacy and Authorship in Nguyen's *New Waves*

In *New Waves,* the character Margo presents a good case study of how online privacy is essentially equivalent to the ability to dictate one's "second self" in the online world. Since Margo is only alive for the first 15 pages of *New Waves*, most of what readers know about her comes from the memories of her friends — all of whom first met her online, as afronaut3000 — and the repository of data that she left behind: her Facebook account, her posts on online platforms, messages to her friends, stories she recorded on her computer, and even her browser history, which clues Lucas in to Margo's activity on Fantastic Planet. And since readers can only learn about Margo post-mortem, through excerpts of the data archives that she left behind and through Lucas' memories of her, a good deal of our understanding of Margo centers primarily

around her position as an author of digital identities, which varied from platform to platform and presented different aspects of Margo operating in different contexts.

As Lucas, her friend in real life, and Jill, a friend she made through their online correspondence on the website Fantastic Planet, compare and reconcile their separate understandings of Margo, the disparity between her real-life identity and the "afronaut3000" identity that she adopted online becomes glaringly obvious. For example, Margo had spoken with both Lucas and Jill about her desire to go to Tokyo. For Lucas, she had only mentioned it few times in passing, and in those conversations, Tokyo was on "a different planet altogether, light-years away."[30] But with Jill, Margo had made concrete plans and spoke about the city as if it was in reach. She had even sent Jill a video on a high-tech burial ground in which she someday wanted to be buried. For Margo, her ability to adopt a new identity freely online allowed her to displace herself. Her "second self" lived in Crown Heights instead of Brooklyn. Tokyo was a hop, a skip, and a jump away, and she could plan a final resting place in a temple with thousands of LED light up Buddhas. Foucault states that the author-function rises out of the distance and division between the actual writer and the fictional narrator, and likewise, afronaut3000 existed as a result of Fantastic Planet's anonymity. The increased degree of privacy that Margo had online gave her a way to literally distance herself from her offline identity, from the body that was later buried in the ground in New York City. The privacy provided by Fantastic Planet is later shattered, though, when Lucas breaches the security of Margo's online accounts; after her digital privacy is invaded, her true identity is revealed to Jill, and the distance between Margo and afronaut3000 is bridged once more. Lucas reveals Margo's name, her height,

[30] Nguyen, *New Waves,* 124.

and her location. He describes the sound of her voice and sends a picture of Margo to Jill. By infringing upon Margo's privacy after her death, Lucas also dismantles afronaut3000, the alternate identity that Margo so carefully crafted while she was alive.

Foucault's theory of authorship applies primarily to the perspective of the user; for adversaries or other third parties from whom we wish to conceal our data and project our chosen representations of ourselves (such as Jill, to whom Margo presents an identity very different from the one she occupies in real life), theories in which the author is entirely absent are a more useful representation of privacy. Roland Barthes argues that "the author enters his own death"[31] at the same moment that writing begins, and that the physical body of the writer should not be tied to the text that is produced. This produces an alternative definition of privacy; in this sense, to have privacy would be to be *allowed* to be born at the same time as one's "text," to have the ability to give no other context to one's "readers," be they other users or Big Tech, without your consent. Privacy, then, is not only Tim's ability to dictate who Amazon thinks he is, but also Tim's ability to be no one else but the identity that he has given Amazon. It is simultaneously the freedom of the author-user to dictate the representation of themselves within their text, and the author-user's non-existence to the rest of the world. This interpretation of privacy as authorship actually reflects the spirit behind differential privacy, since differential privacy defines adjacent databases as databases that differ by one individual (either with this individual removed or swapped out for another) and demands that the outputs of the algorithms run on these adjacent databases be indistinguishable. In some sense, this definition can be regarded as (0,0)-

[31] Roland Barthes, "The Death of the Author," in *Twentieth Century Literary Theory, (*New York: Macmillan ; St. Martin's Press, 1997), 120.

differentially private since the goal is for the contribution of the individual in question to be fully indistinguishable from either its complete absence or replacement.

This framing of privacy and authorship as understood by Barthes helps us to better understand exactly what Lucas does when he exposes the real person behind afronaut3000 to Jill; Lucas forces Jill to see afronaut3000 as Margo, a person with a biography, a height, an ethnicity, and a background. afronaut3000's re-identification renders Margo the simplistic, biographical kind of author that Barthes is hoping "dies," and deprives Margo's "work" (the aggregate of her activity on Fantastic Planet) of the anonymity it once had. In this sense, Lucas destroys both Margo's authorship and her privacy not only by bridging the gap between her real identity and the second self that she created, but also by exposing the individual behind the work produced.

Meanwhile, the idea that Margo's authorship is inextricably linked with her personal privacy is reinforced by Margo's status as an author in the traditional sense of the word. After Margo's death, Lucas and Jill discover hundreds of audio files saved locally on her laptop, hidden in a folder named "Fantastic Planet." All of them are verbal short stories, recorded by Margo. Despite the fact that the folder is named Fantastic Planet, there is no evidence that Margo ever shared or published these stories, unlike Jill, who shared her novel, *Mining Colony*, with Margo through the Fantastic Planet platform. Whereas many people who use social media or other forms of self-publication online feel the need to portray themselves positively, Margo takes advantage of the privacy afforded by never sharing her stories to craft her own narratives, which, as Lucas points out, all have a "dark, cynical plot twist."[32] In one story, there is a designated authority that solves all the problems of the world, but that authority figure gives up on humanity

[32] Nguyen, *New Waves,* 134.

and decides to effectively end the world. And though that particular story is ostensibly about climate change and extinction, Margo expresses frustration with authority and semantics by criticizing "pollution" as a "great euphemism," used "when really what we mean is the consequence of humanity."[33] Margo's privacy facilitates her ridicule of the societal norms that frustrate her most in her life as a female engineer: traditional gender dynamics, corporate culture, climate change, authority, and semantics. Her privacy allows her to completely own her creative voice and to express her deepest frustrations through her short stories. It allows her to slip up from time to time and finish a story with tipsy laughter, to drunkenly rant about the worst of humanity and to burp between sentences.

Margo's critiques of society are as deeply effective and scathing as they are due to her extensive use of defamiliarization. As Viktor Shklovsky writes in "Art as Technique," "as perception becomes habitual, it becomes automatic… the purpose of art is to impart the sensation of things as they are perceived and not as they are known."[34] Defamiliarization is thus a technique that introduces "a novel point of view," which "can make a reader perceive by making the familiar seem strange."[35] By setting her stories in unfamiliar futures and writing about despicable, pitiable characters while maintaining the existence of the problems that bother her the most in her daily life, Margo forces her listeners to de-automatize their perception of societal norms, which in turn allows them to see the artifice and absurdity of these standards. For example, two of Margo's stories are set on extraterrestrial planets; one planet is the refuge of the last two survivors of humanity after Earth explodes, and the other is Mars, where, in Margo's

[33] Nguyen, *New Waves*, 195.
[34] Viktor Shklovsky, "Art as Technique" in *Russian Formalist Criticism,* (Lincoln: Nebraska Paperback, 2012), 11-12.
[35] Ibid, 5.

constructed world, humanity has set up a new colony. In the first story, the one surviving man attempts to force the one surviving woman to stay and build a life with him, as part of their duty and responsibility to "continue the existence of the human race," to be "father and mother to a new generation."[36] In response, the woman leaves the man behind and "sets off toward the jungle to live her own damn life."[37] This story triumphantly points out the arbitrary nature of human constructions like duty, responsibility, and marriage, and it establishes that in a newly created vacuum, none of the above are necessary. On the other hand, the second story set on Mars features a young woman who is eventually imprisoned after shooting her stalker in an act of self-defense. The conclusion that Margo comes to is that "Mars is just like any other planet: a giant mass of garbage that orbits through space, barely able to sustain human life."[38] This story differs greatly from the other in that a new planet is not a new beginning for humanity, but Margo still manages to condemn sexism and misogyny as that which renders this new world "a giant mass of garbage." And so, Margo uses the technique of defamiliarization to undermine the authorities and institutions that cause her grief in her day-to-day life, and her uncensored form of rebellion is enabled precisely because of her platform's privacy.

Conclusion

Therefore, though there are already a variety of existing technical and legal definitions of privacy, none are complete. But by interpreting users as congruent to authors who produce online data instead of texts, we can define privacy as a form of authorship, in which true privacy is the freedom of the author to shape their "second self" as they please. And so, complete privacy

[36] Nguyen, *New Waves*, 17.
[37] Ibid.
[38] Ibid, 138.

allows users to act as uncensored authors of their works, or rather, to explicitly control the many representations of themselves online without any limitations. It is certainly not the paradigm that the world currently operates under, but whether or not it *should* or *could* be are entirely different questions.

Meanwhile, Margo's writing and use of defamiliarization illustrates the effectiveness of exploring contemporary issues through the lens of fiction, which this thesis aims to do as well, specifically for issues of privacy. As Fredric Jameson argues in "Progress versus Utopia or, Can We Imagine the Future?", imaginary depictions of the future serve "to defamiliarize and restructure our experience of our own *present*."[39] And so, in the next chapter, as I discuss these questions of whether or not complete privacy is realistic or even desirable, I continue analyzing real-life scenarios in tandem with speculative fiction.

[39] Fredric Jameson, *Archaeologies of the Future: the Desire Called Utopia and Other Science Fictions*, (London ; New York: Verso, 2005), 286.

Chapter 2: Tradeoffs and the Tech Gothic

As I argued in the previous chapter, digital privacy offers online users a greater degree of autonomy and dignity; it allows them to preserve their sense of independence and self and to dictate the ways in which they choose to portray themselves to different entities. Unfortunately, privacy is oftentimes at odds with other benefits that society desires from technology, such as convenience, personalization, security, and accountability. Striking a balance between these other benefits and privacy is a difficult task, made all the more complicated by the competing priorities of different stakeholders.

Speculative Fiction as Edge Cases

When testing new code or algorithms in computer science, it is common practice to test edge cases to see if a given system or mechanism is comprehensive enough to handle all types of inputs, and not just expected cases; outliers test conceptual frameworks by stressing them to an extent that normal cases cannot. In some sense, this is also the purpose of speculative fiction: to explore the hyperbolic "edge cases" that we have yet to enact in real life, to predict new catastrophes, and to investigate the consequences of various proposed crises. And yet, while computer scientists might be more interested in evaluating the plausibility of these explorations, I argue that they are important regardless of their likelihood of manifesting in real life. Fictional worst-case scenarios and dystopic societies conjured by contemporary authors may occur with fairly low probability, but they are still the products of contemporary social anxieties and fears. As such, I believe that examining fictional stories with exaggerated plots is a valuable exercise

that may teach us about fundamental issues we face in our society today. Fiction defamiliarizes these issues and so allows us to perceive them with fresh eyes.

Little Brother by Corey Doctorow, *New Waves* by Kevin Nguyen, and *The Circle* by Dave Eggers are all examples of speculative, "edge case" novels. *Little Brother* explores the possibility of an accelerated surveillance arms race in a large, American city following a terrorist attack. *New Waves,* on the other hand, proposes a privacy-forward messaging application run by a small startup that gets severely abused by malicious users; the eventual solution turns the messaging application into a heavily moderated communication system with no nuances or loopholes to preserve user privacy in any way. And finally, the world of *The Circle* is interesting in that many of the characters genuinely believe that they are building a utopia — their technologies allow for greater levels of convenience, transparency, online accountability, safety, comprehensive healthcare, and access to voting. But privacy is almost always the cost paid for these benefits, and it is widely regarded as a flaw and not a feature. Therefore, *The Circle* offers a dystopian vision of a near-future America governed entirely by Big Tech, in which an attempt to preserve one's privacy is equivalent to opting out of society completely.

Defining the Tech Gothic

Using these three novels, I theorize a new genre called "tech gothic," which adapts the genre of gothic literature to the new, high-tech landscape of modern society to expose its hidden horrors. The signature locale of a "gloomy castle furnished with dungeons, subterranean passages, and sliding panels"[40] has been replaced by cities bedazzled with a wide array of

[40] M. H. Abrams and Geoffrey Galt Harpham, "Gothic Novel," in *A Glossary of Literary Terms* (Australia: Cengage Learning, 2015), 111.

surveillance technology, the small but trendy office space of an emerging startup, and the sprawling, cutting-edge work campus typical of Big Tech. The traditional gothic plot focused on "the sufferings imposed on an innocent heroine by a cruel and lustful villain"[41] remains more or less intact, but the villains have been replaced by controlling entities that want to police the actions of society by aggregating personal data (governments and technology conglomerates), and the protagonists have become people who operate outside of the traditional hierarchies of power in tech culture (rebellious schoolchildren, female engineers, and customer service representatives). And finally, there is still an omnipresent, mysterious power that torments the main character; the threats of violence, exposure, and surveillance persist, but the means are now technological instead of supernatural.

Little Brother, New Waves, and *The Circle* are all examples of tech gothic literature. *Little Brother* tells the story of Marcus, a high school student living in a heavily surveilled, near-future San Francisco. In "proactive enforcement programs,"[42] the government uses technology to monitor mundane aspects of life: cameras are installed in every classroom at Marcus's school, every purchase made with a debit or credit card is tracked, and every person's public transit use is monitored by the Department of Homeland Security (DHS) so that individuals with "suspicious profiles" (unusual travel patterns) can be identified and questioned. The surveillance experienced by Marcus and his community is newly implemented and motivated by the fear of terrorism, since the city has just suffered a major terrorist attack. And yet, the fear that pervades the novel is not of terrorism, but rather that of government surveillance and police brutality. At the beginning of the novel, Marcus and a few of his friends are deemed "suspicious" by the DHS

[41] Abrams, *A Glossary of Literary Terms,* 111.
[42] Cory Doctorow, *Little Brother*, (New York, NY: Tor Teen, 2008), 108.

for being near the site of the terrorist attack when it occurs. They are forcibly detained, interrogated, shackled, imprisoned, beaten, drugged, and even waterboarded. When Marcus is finally released, an agent from the DHS tells him, "From now on, you *belong* to us. We will be watching you. We'll be waiting for you to make a misstep. Do you understand that we can watch you closely, all the time?"[43] This threat, coupled with the increased police presence throughout the city and the newly installed surveillance technology, echo the gothic motifs of omnipresent danger and fear, though the DHS's near omniscience is enabled by technology instead of supernatural forces. Marcus, in turn, serves as the counterpart of the innocent gothic heroine at risk; he and his cohort of hacktivists are, for the most part, school-aged children, who are constantly being sought out, threatened, and arrested by DHS agents.

Meanwhile, *New Waves* reflects many of the tech gothic genre's defining features in that it is set against the backdrop of a small startup where Lucas and Margo work, called Phantom (which mirrors the aesthetic of the gothic genre in its name alone). The product that their company produces is a platform for sending messages that are quickly deleted. Margo, as a female engineer, and Lucas, as the only customer service representative employed at Phantom, are marginalized by the culture of their company, and through their marginalization and relative powerlessness, resemble the stereotypical protagonists of gothic literature. And although Lucas' physical safety is never threatened by any entities within the novel, he becomes haunted by Margo — for though she dies, her data lives on. Phantom, too, with its ephemeral messages, functions as a ghostly presence throughout the novel, and its weaponization at the hands of cyberbullies turns it into a genuine threat and platform for perpetrating harm.

[43] Doctorow, *Little Brother*, 64-65.

The Circle is set in a hypothetical future in which a major tech company called the Circle has come to control all aspects of life. The events of the novel take place in the posh headquarters of the Circle, which features a wide variety of amenities and functions in a manner reminiscent of the Googleplex or other famous Big Tech offices. The protagonist of *The Circle* is Mae, a new customer service employee at the Circle who is perpetually surrounded by the company's technology and threatened by it; her work is evaluated not only by the quantity and quality of her replies to customer inquiries, but also by her participation in the Circle community via social media, both within the company's internal system (the InnerCircle) and on the company's external social media platform (referred to as the OuterCircle by employees). (Evocative of the Inner Party and Outer Party of George Orwell's *Nineteen Eighty-Four*, these names highlight the connections between the gothic and dystopian genres that have been noted by scholars including Sherryl Vint.)[44] The social media takes up a third screen on Mae's desk, and it feeds her "forty new InnerCircle messages every few minutes, fifteen or so OuterCircle posts and zings,"[45] occupying "every available moment of downtime"[46] for Mae. Her location on the Circle's campus is tracked continuously, attendance at social events is effectively mandatory (as are social media posts about each event she attends), and soon, the number of screens on her desk increases to five, along with a headset that asks her to verbally respond to survey questions (of which there can be five hundred in a single hour). Therefore, Mae's position in the company is surprisingly precarious, and the omnipresent power of the Circle is constantly with her for every moment of the day — this becomes quite literal after Mae goes "transparent," and

[44] Sherryl Vint, "Dystopian Science Fiction and the Return of the Gothic," in *The Oxford History of the Novel in English: Volume 7: British and Irish Fiction Since 1940*, ed. Peter Boxall, and Bryan Cheyette (Oxford: Oxford University Press, 2016), 384–398.
[45] Dave Eggers, *The Circle: A Novel* (New York: Vintage Books, 2014), 105.
[46] Ibid.

essentially livestreams every waking moment of her life to tens of thousands of viewers. And so, *The Circle* exemplifies many of the gothic genre's defining features — a setting of a high-tech corporate campus, a young and impressionable heroine in danger, as well as the constant, watchful, and unsettling presence of a powerful entity — translated to fit within the ecosystem of Big Tech.

The gothic genre famously "develops a brooding atmosphere of gloom and terror" and exposes the "nightmarish terrors that lie beneath the orderly surface of the civilized mind."[47] Tech gothic also develops this same, terrifying atmosphere, but it does so by drawing on pre-existing social anxieties and fears within contemporary society regarding technology. *Little Brother, New Waves,* and *The Circle* all deal with privacy and the difficulty in balancing privacy with other benefits to society. Thus, they expose the fear and struggle surrounding the various underlying tradeoffs that governments, developers, and consumers must make in trying to preserve privacy.

Examining a Tradeoff: Privacy vs. Surveillance and Security

While Harvard students, faculty, and employees rarely think of themselves as living and working within the setting of a tech gothic, the campus and its surroundings are highly surveilled. There are at least 1100 security cameras between the Charles River and the former engineering school at Harvard. There are 200 in the Art Museum alone. There is at least one in each of the buses that circle Harvard Square, and eight in the little falafel shop by the Kennedy School. Foucault calls this inescapable surveillance "a compact model of the disciplinary

[47] Abrams, *A Glossary of Literary Terms,* 111.

mechanism."[48] According to Foucault, surveillance plays a *disciplinary role* in society. Security cameras, for example, allow us to not only identify lawbreakers, but also help to prevent laws from being broken in the first place, since no one wants to be recorded committing a crime. This is a manifestation of Foucault's "utopia of the perfectly governed city,"[49] one way in which our society exercises power over its citizens.

However, this increased level of safety and security comes at a cost to personal privacy. At what point is the security provided by more surveillance too invasive to be "worth it"? And at what point is so much privacy afforded to individuals that dangerous behavior is enabled, and members of society are put at risk? Cory Doctorow explores this tradeoff in *Little Brother*, demonstrating that the theoretical benefits of surveillance can fall apart in practice. The Department of Homeland Security's public transit surveillance system does not succeed in catching any terrorists, for example; instead, it haunts the citizens of the city, busting cheating spouses and lying children. This is an example of the "paradox of the false positive," which Marcus explains in his internal monologue as he looks for a way to exploit the city's public transit surveillance.

The paradox of the false positive is best explained through example, which Marcus provides. Let us assume as Marcus does, that in a city of 20 million like New York, there are at most 10 terrorists. That means, of the entire population, 0.00005% of people are terrorists. Now, let us assume that there is a miraculous algorithm capable of identifying terrorists with 99% accuracy. But then running this algorithm on the entire population of 20 million citizens will

[48] Michel Foucault, ""Panopticism" from "Discipline & Punish: The Birth of the Prison"" in *Race/ethnicity: Multidisciplinary Global Contexts* (Ohio State University: 2008), 3.
[49] Foucault, "Panopticism," 4.

yield 200,000 individuals identified as terrorists, of which at most 10 are guilty. Because the accuracy of the test does not match the rarity of the occurrence itself, the false positive results lead to massive collateral damage: at least 199,990 innocent people interrogated and investigated. We can also calculate the probability that a person is actually a terrorist given that they have been flagged as "suspicious" by using the definition of conditional probability:

$$T = \text{Is Terrorist}, F = \text{Is Flagged}$$
$$Pr(T) = \frac{10}{20,000,000} = 0.0000005$$
$$Pr(T \cup F) = 0.99 * Pr(T) = 0.000000495$$
$$Pr(T' \cup F) = 0.01 * (1 - Pr(T)) = 0.009999995$$
$$Pr(T|F) = \frac{Pr(T \cup F)}{Pr(T \cup F) + Pr(T' \cup F)} \approx \boxed{0.0000495}$$

And so, the probability that a person is actually a terrorist given that they have been flagged is ridiculously low, which means we must flag and interrogate a disproportionately large number of people (nearly all 20 million) in order to find the 10 terrorists. Therefore, implementing a surveillance system that classifies people as suspicious with accuracy less than the rarity of the occurrence itself is remarkably inefficient and impractical; it will only serve to threaten innocent bystanders, like Marcus, who is cornered by policemen waiting outside a subway station for him. By explaining the math behind the paradox of the false positive and demonstrating that the government will likely detain and harass many innocent people at random, *Little Brother* creates a sense of gothic foreboding, and by describing the impact of the paradox on Marcus and other everyday citizens within San Francisco, the novel makes this theoretical problem feel very real and terrifying.

As Marcus writes on his Xnet site, "The important thing about security systems isn't how they work, it's how they fail."[50] When he attempts to subvert the surveillance system, Marcus inadvertently begins an arms race between independent hacktivists and the Department of Homeland Security. After Marcus is apprehended as one of the many false positives reported by the system, he devises a way to swap transit profiles with strangers as they pass by, so that the system attributes their travel activity to the wrong person. This method, later called "jamming," becomes widespread amongst users of Xnet, an independent mesh network. Jamming helps to misrepresent one's movement to the government, and therefore offers people a little bit more control over their personal privacy; however, since it also misrepresents someone else's movements to the government without their knowledge, it is problematic in terms of *their* privacy, authorship, and consent, as well. But despite its problematic nature, jamming essentially allows Marcus and the other Xnetters to begin randomly distributing ride profiles throughout the city, which exacerbates the problems already caused by the paradox of the false positive.

Little Brother also demonstrates that any amount of surveillance will not be sufficient so long as the people being surveilled are aware of it. Marcus — as well as the other Xnetters — are the unintended adversaries of the Department of Homeland Security's surveillance. Jamming is their first innovation, but since the Department of Homeland Security does eventually figure out a way to counter it, Marcus responds by writing on his blog, "They figured out how to stop our tactic, so we need to come up with a new tactic."[51] He advocates *against* jamming and for new tactics, and the Department of Homeland Security becomes engaged in a technological arms race against Xnetters. The adversaries of their system are no longer terrorists, but the very civilians

[50] Doctorow, *Little Brother*, 126.
[51] Ibid, 244.

that they were initially supposed to protect, and the government replaces the terrorists as the source of omnipresent paranoia, terror, and fear.

In some sense, the arms race seems like it could be beneficial, since any surveillance or security system that can be so easily overturned is pointless. As Marcus points out, "Jamming proves that they can't fight terrorism because it proves that they can't even stop a bunch of kids."[52] However, governments around the world have taken a very different approach; many of them place boundaries on non-government encryption through legislation or court cases. This does, in a sense, stop the arms race, and it counters the intended adversaries — terrorists, school shooters, pedophiles — by giving them fewer fully developed, easily accessible tools to work with. Unfortunately, this particular approach also means that everyday civilians, businesses, and at-risk groups (like journalists, activists, or marginalized groups who fear persecution) have fewer tools with which to protect their personal privacy.

In the United States, at least, strong encryption in the hands of non-government entities has always made the government uneasy. Over the years, as technology has advanced and strong encryption has become more widespread and available, the conflict between national security and strong encryption has escalated. The government has attempted to intervene on multiple occasions, which has led to a long-term conflict unofficially dubbed the "Crypto Wars." For example, in the late 1970's, a new symmetric key encryption algorithm, DES, was introduced. IBM had originally planned to use a key size of 64 bits, whereas the NSA wanted them to use a key size of 48 bits instead. The reduced key size would have decreased the cost of attacking the cryptosystem. Ultimately, IBM and the NSA settled on a compromise that involved the use of

[52] Doctorow, *Little Brother*, 245.

parity bits, which effectively reduced the key size to 56 bits.[53] While a 56-bit sized key is certainly more secure than one with 48 bits, it is certainly not as effective as 64 bits would have been, since the addition of each extra bit makes the key twice as hard to crack. Therefore, this is a clear instance in which the government interfered in the development of a privately owned encryption algorithm and actually succeeded in weakening it.

The most famous instance from recent years in which the government attempted to interfere in a privately owned encryption is the FBI-Apple encryption dispute. In 2015 and 2016, Apple received several orders from American district courts attempting to force Apple to assist the government in extracting data like contacts, photos, and calls from locked iPhones.[54] Given that some of the devices had more extensive security protections, the orders would have compelled Apple to write new software to aid the government in bypassing these device's security. The most well-known case of this was a February 2016 case in which the FBI wanted Apple to aid them in unlocking an iPhone recovered from one of the shooters from the San Bernardino shooting, who had killed 14 people and injured 22. Apple opposed the court order they had been given, and a hearing was scheduled in March before it was called off since the FBI had found another way to unlock the contents of the phone. And so, the case was never resolved; while Apple was not forced to build a backdoor for their system, the U.S. government may very well attempt to coerce technology companies to compromise the security of their products in the future. Many of these cases are litigated in secret, so there may very well be more developments

[53] Henry Corrigan-Gibbbs, "Keeping Secrets," Stanford Magazine (Medium, November 7, 2014), https://stanfordmag.medium.com/keeping-secrets-84a7697bf89f.
[54] Jenna McLaughlin, "New Court Filing Reveals Apple Faces 12 Other Requests to Break into Locked Iphones," The Intercept, February 23, 2016, https://theintercept.com/2016/02/23/new-court-filing-reveals-apple-faces-12-other-requests-to-break-into-locked-iphones/.

to come in the next few years, but for now, the Crypto Wars in the United States remain unresolved.[55]

Fortunately, however, this does mean that the effort to establish a working compromise between privacy and security is ongoing. In 2019, a group comprised of former government officials, business representatives, privacy and civil rights advocates, law enforcement experts, and computer scientists came together to seek common ground and to "promote a more pragmatic and constructive debate on the benefits and challenges of the increasing use of encryption."[56] They identified a list of strategies conducive to more constructive dialogue between stakeholders, including avoiding absolutist positions, framing the debate as a shared concern, accepting imperfection, and separating the debate into components (for example, categorizing data into several categories, like data in the cloud, data in motion, and data on devices) to address them one at a time. While this coalition focused in particular on mobile phone encryption, these strategies are applicable to other devices and platforms as well.

Little Brother highlights the difficulty in making this tradeoff between privacy and security and gives readers a glimpse of a terrifying future in which a compromise is never reached. While surveillance is an important tool in keeping communities safe, increasing surveillance also edges communities closer and closer to the horrifying world forecast by the tech gothic. There is no right or easy choice — but hopefully, by making use of strategies like

[55] Real World Crypto, "Real World Crypto conference 2020: session 4," Youtube, February 13, 2020, https://www.youtube.com/watch?v=_CpjIFh0Kis.
[56] Encryption Working Group, "Moving the Encryption Policy Conversation Forward," Carnegie Endowment for International Peace, September 10, 2019, https://carnegieendowment.org/2019/09/10/moving-encryption-policy-conversation-forward-pub-79573.

the ones identified by the multi-party coalition in 2019, a compromise can eventually be established.

Examining a Tradeoff: Privacy vs. Accountability in Messaging Systems

In *New Waves,* readers encounter an entirely different privacy tradeoff in the form of Phantom, the startup that Lucas and Margo work for. Their primary product is a platform for sending messages that are quickly deleted, and while the original intention was for their product to be a way for whistleblowers to reach out to others without fear of leaving behind evidence, Phantom becomes overrun with malicious users — primarily teenagers — sending explicit messages to and harassing each other. *New Waves* is a tech gothic novel that demonstrates the unfortunate potential that privacy has to enable malicious behavior; by granting users privacy through transience, Phantom enables users to become "phantoms" themselves, to replace the malevolent, supernatural ghosts of gothic literature by haunting others through technological means. When victimized users begin contacting Lucas for help, the most he can do is help them block the sender. Given that the messages are ephemeral, Lucas is unable to verify that screenshots of the abusive behavior are real, and Phantom cannot penalize the alleged sender of the messages or hold them accountable in any way.

The solution that Phantom eventually comes to is not only ineffective but also highly invasive of their user's privacy. Due to public pressure and news coverage of an incident in which a high school student is viciously bullied, Phantom begins monitoring messages for inappropriate content, at a cost to user privacy. The company's procedures for monitoring messages are labor-intensive, inefficient, ineffective, and not privacy-preserving at all; while

messages appear to be ephemeral to other users, they are saved and sifted through by hired content moderators. Phantom eventually trains a machine learning model to auto-flag suspicious messages (once again, using data that should not have been saved for purposes that users did not consent to) to feed to content moderators, but since the system is only capable of flagging abusive language, users began sending image links with explicit, hateful, and Nazi imagery. To counter their accounts being flagged, malicious users simply make new ones and continue to threaten their victims — the ghosts continue to haunt. As Lucas claims, "it was a Band-Aid when we needed stitches."[57] For Phantom, accountability comes entirely at a cost to user privacy, and it is not even effective.

The need to balance accountability and privacy is not a problem exclusive to fictional messaging platforms, as demonstrated by the different approaches taken by Signal and Yik Yak. Signal preserves privacy through its end-to-end encryption scheme; it is very difficult for anyone apart from the sender and recipient to read the decrypted contents of any message. Apart from knowing when messages are sent and between whom, Signal itself has literally no other information. As such, users cannot be easily held accountable for the content of their messages. However, unlike Phantom, Signal does have a barrier of entry to making new accounts; each Signal account requires a new and distinct phone number without an account already associated with it, which means that users cannot bypass blocking or harass others under different pseudonyms quite as easily. On the other hand, Yik Yak was an anonymous social media app launched in 2013 that allowed people to create discussion threads and view them within a 5-mile radius. The app was monitored by the community, and users were able to downvote posts that

[57] Nguyen, *New Waves,* 115.

people found offensive. If a post received enough downvotes, it would be removed. However, the privacy policy required a subpoena, court order, or search warrant to identify users who posed a risk. As a result, Yik Yak became criticized for facilitating cyberbullying; those who used Yik Yak's anonymous messaging capabilities to harass those around them could not be apprehended easily.[58] Therefore, like Signal, Yik Yak's users could not easily be held accountable for messages sent using the platform. Both Signal and Yik Yak preserve the privacy of their users far more than Phantom, but the additional degree of protection is not without cost.

Meanwhile, in August 2021, Apple attempted to introduce new technical measures in Messages, iCloud, Siri, and search to protect children from sexual abuse. Like Phantom in *New Waves*, they did seem to think that content moderation would be the solution, though their proposed protocol was significantly more sophisticated. Instead of scanning images directly to look for child sexual abuse materials, they compared cryptographic hashes of user data with cryptographic hashes of known abusive images; in this way, they didn't have to look directly at user data.[59] However, these features were recalled by Apple after backlash from cryptographers and privacy advocates. Apart from technical issues like potential false positives, advocates were worried that any system used to scan for specific types of content could easily be repurposed into a tool for wider surveillance. Likewise, privacy advocates were also against the content moderation system simply because they were afraid that it would normalize the notion of being

[58] Valeriya Safronova, "The Rise and Fall of Yik Yak, the Anonymous Messaging App," The New York Times (The New York Times, May 27, 2017), https://www.nytimes.com/2017/05/27/style/yik-yak-bullying-mary-washington.html.
[59] Brian Barrett, "Apple Backs down on Its Controversial Photo-Scanning Plans," Wired (Conde Nast, September 3, 2021), https://www.wired.com/story/apple-icloud-photo-scan-csam-pause-backlash/.

surveilled, despite the effort that Apple made to scan the images indirectly and to preserve user privacy.

Therefore, in *New Waves*, Nguyen anticipates a new version of privacy-forward messaging, in which ephemerality is the mechanism by which users can protect themselves instead of end-to-end encryption or anonymity. Private messaging is crucial for people to protect themselves, to conduct business, and to maintain the ability to represent themselves in the ways that they choose to different entities. *New Waves*, however, demonstrates how insufficient methods of holding users accountable and how abuse of technology can make the preservation of user privacy foundational to the tech gothic. Technology once again replaces supernatural forces as that which enables users to perpetrate harm. Like *Little Brother*, *New Waves* presents a worst-case scenario in which the solution to abuse completely defeats the purpose of the messaging service to begin with and thus demonstrates the consequences of failing to achieve a sufficient balance between privacy and accountability. This struggle to find a compromise between privacy and accountability will likely stay relevant as the demand for private messaging increases; similarly, the struggle to implement content moderation in a privacy-preserving way will also remain so long as malicious users like terrorists and pedophiles take advantage of private messaging.

The Necessity of Tradeoffs

Despite the difficulty of navigating these various privacy tradeoffs, the fact that they actually exist is a relief. *The Circle*, as the most extreme tech gothic novel among the three discussed in this thesis, explores the fear of completely giving up on privacy in favor of the benefits that can be reaped without it. The protagonist, Mae, initially begins in customer service

but rises quickly through the company's ranks by creating and promoting the axioms "Secrets are lies," "Sharing is caring," and "Privacy is theft." These axioms explicitly reference George Orwell's *Nineteen Eighty-Four,* and this allusion emphasizes the menacing atmosphere of the Circle and contributes to its tech gothic sensibility. The Circle's primary product is TruYou, which allows users to aggregate all their online needs on a single platform. The company makes a wide variety of other products as well, like trackers that can be embedded in children's bones to keep them safe from kidnappers, cameras that livestream high-quality surveillance video at all times, and deep-sea submarines for exploring the Mariana Trench. All of these products offer amazing improvements to quality of life by making their users' lives easier and safer or by pushing the boundaries of scientific knowledge. However, many of these products also refuse their users any agency at all over the way they are represented — not only to the company itself but also to other users of Circle products — and therefore constitute a massive invasion of user privacy.

One Circle product based entirely on the violation of another individual's privacy is LuvLuv, which allows people to search for information on potential dates to help them better understand their specified individual. It is marketed as a helpful tool for picking out date activities and getting to know a potential partner; by scanning old internet archives, social media posts, and information collected by the Circle, it provides information on a person's allergies, interests, hobbies, and preferences. It even analyzes the person's TruYou payment history and generates reports on their restaurant visit history and the dishes they ordered at each restaurant. Francis — Mae's love interest in the novel — participates in a demonstration of LuvLuv at work and searches for Mae's information in front of an entire crowd. Mae is mortified, though she struggles to identify why. All of the information revealed in the demonstration is publicly

available, and a good deal of it is posted by Mae herself; one of LuvLuv's primary functions is to aggregate and parse all online records of a person, including their social media profiles and usage. Mae comes to the conclusion that LuvLuv made her uncomfortable because the results were "some kind of mirror, but it was incomplete, distorted."[60] By resorting to LuvLuv instead of directly asking Mae about her preferences, Francis deprived her of her opportunity to dictate the way in which she would like to represent herself, and this twisted representation of Mae is revealed not only to Francis but also to everyone else at the Circle who witnessed the LuvLuv demonstration. Apart from the fact that LuvLuv could easily be abused by malicious entities — say, stalkers, instead of potential dates — it replaces the traditional manner in which people usually get to know each other. Even with the presence of social media, other humans are incapable of efficiently aggregating and analyzing data like LuvLuv, so people are normally given the chance to express themselves and reveal information at a pace they prefer. But LuvLuv can generate profiles on anyone who uses any Circle products — regardless of whether or not they use LuvLuv or give consent in any way — thereby invading their privacy. In this sense, Eggers's portrayal of LuvLuv draws on traditional gothic motifs in which romance becomes dangerous and threatening by removing consent from the equation and taking control away from Mae and other Circle users. So while LuvLuv does lessen the anxiety of picking a perfect spot for a first date, it also fundamentally changes the nature of human interaction and violates the privacy of Circle users by dictating their representations of themselves.

Another Circle product based entirely on the violation of an individual's privacy is Francis's pet project, ChildTrack, which is later renamed TruYouth. It is a location-sharing chip

[60] Eggers, *The Circle*, 126.

designed to be embedded in a child's bone so that it cannot be easily removed, and it notifies authorities "the second a kid's not where he's supposed to be."[61] Once again, in the description of this technology, Eggers draws upon motifs of traditional gothic literature — skeletons and bones — and combines them with haunting surveillance to convey the terrifying potential of this technology. To implement TruYouth would require not only real-time location data for all underage children, but also data about a child's usual routine and location. Furthermore, TruYouth shares all of this information with government authorities. Given that the chip is embedded in the bone and that location-sharing is constant, this is not something that either children or guardians have the ability to opt out of for any duration. While Francis calls this "a new golden age for young people" and "an age without worry,"[62] this would also be an age in which any minor who takes an unplanned walk around the block could have the police descending down upon them in less than a minute and a half — the length of time that an abductor would have to run away with a child under TruYouth's surveillance, according to Francis. Additionally, since children likely behave in unexpected ways far more frequently than they are kidnapped, the accuracy of TruYouth seems like it would be quite low; the paradox of the false positive suggests that, for the vast majority of children, TruYouth would not be an effective method of preventing child abduction. Instead, TruYouth would be nothing other than surveillance, a way to enforce the routine shared with the government. Furthermore, since TruYouth requires that both the government and the Circle have information on a child's location, there is no guaranteeing that this data is not misappropriated for other uses, like customizing advertisements or helping authorities arrest the child should they commit a crime.

[61] Eggers, *The Circle*, 90.
[62] Ibid.

For all we know, the next generation of children who live with TruYouth could have their childhood memories incorporated into their LuvLuv profile. While none of this seems like a drawback on the surface, it does take agency away from both children and guardians while inviting interference from the government and the Circle in daily life for a vulnerable population. Apart from severely impacting their lives in the case of a false positive, TruYouth deprives children and families of the opportunity to selectively reveal their personal location information to the Circle and the government, which constitutes a violation of their privacy. But once again, since the Circle believes that "Secrets are lies," "Sharing is caring," and "Privacy is theft,"[63] these aspects of TruYouth would likely seem like features and not flaws to Mae and her colleagues.

Meanwhile, the Circle's internal data sharing practices are extremely concerning and violate Circle users' privacy by assuming automatic consent to the many ways in which their data is used. Mae has an incident in her second of week of work in which she is reprimanded for not responding to a coworker's invite to a Portugal-themed brunch. Mae has no desire whatsoever to attend the Portugal brunch in the first place, though she later finds out that she was likely invited because she took pictures 5 years prior during a trip to Lisbon. The pictures were saved on her laptop, which then uploaded that information to the cloud. When Mae's coworker, Alistair, organized the brunch, he likely did a campus-wide search for individuals with connections to Portugal, and Mae was included because of her photos. While Mae's frustration following the incident is due in part to her awkward meeting with Alistair, she also has genuinely no idea why she had been invited to this brunch. In trying to save her photos from her trip to

[63] Eggers, *The Circle*, 305.

Lisbon, she had not intended to show her colleagues and the rest of the world that she had a lifelong interest in Portugal. Mae never gave consent for her data to be used in this way, and the Circle's automatic uploading to the cloud, as well as all the other Circle employee's ability to access it, has once again restricted Mae's ability to misrepresent herself, to construct the image that she shares with the rest of the world. In return, people like Alistair looking to find specific subpopulations of people for events have a much easier time. Mae's privacy is sacrificed for someone else's convenience.

However, Mae's missed Portugal brunch is not only an issue of consent, but also an issue of retention. Mae's trip to Lisbon was five years before she began working at the Circle, and yet, photos from this time were still considered in generating a report of Mae's interests and affiliations. The Circle has a habit of not only aggregating all of the data it can from different products — like how LuvLuv makes use of payment histories created through TruYou — they also tend to keep the data around forever. While many companies today have set retention periods for personal data (due to the European Union's General Data Protection Regulation), the Circle attempts to retain all data in perpetuity. As Gus mentions in his demonstration of LuvLuv, the Circle supposedly purchased all of Facebook's user data after putting it out of business, and Annie tells Mae that "we don't delete here… it's like killing babies."[64] For Mae, specifically, this is problematic because of an explicit video that Francis recorded of her without her knowledge. Many gothic plots involve some sense of sexual violation for the heroine, and the repetition of this motif within a technological context helps to demonstrate the severe consequences of the

[64] Eggers, *The Circle*, 206.

Circle's data retention practices in a way that feels visceral, uncomfortable, and genuinely terrifying.

This incident is also related to the U.S.'s primary case with the right to forget; just as terrorists and pedophiles drive the government's position on prioritizing security over privacy, the battle against data retention in the United States has revolved primarily around revenge porn. But since the Circle's data archives function as an "official record" of the self (as the results of a Google search might today), Mae and the other citizens of Eggers's world have no say in what the rest of the world knows about them.

Therefore, as difficult as tradeoffs are, it is perhaps a good thing that they still exist in our current society. We cannot require technology corporations or governments to grant users complete privacy, nor is allowing them full reign over user data a good idea; as demonstrated by *Little Brother, New Waves,* and *The Circle,* a skewed balance or a single entity with too much control can have terrifying repercussions for users and pushes us closer into the world of the tech gothic. A line must be drawn somewhere.

Drawing the Line

Different stakeholders all have different priorities, and as such, every entity draws their lines of comfort quite differently. But in a world without impartial arbitrators, we must collectively attempt to reach a universal agreement. The strategies used to address the Crypto Wars are ones that can be adopted to navigate all of the tradeoffs discussed in this chapter — we must accept imperfections, avoid absolutist positions, seek common ground, and address issues one component at a time.

Helen Nissenbaum's *Privacy in Context: Technology, Policy, and the Integrity of Social Life* defines a "framework of contextual integrity" which is also helpful in establishing a goal for privacy practices; she argues that it is more important to ensure that the flow of information between people and entities is *appropriate,* instead of restricted altogether. She claims that there exist "finely calibrated systems of social norms" that "govern the flow of information in distinct social contexts,"[65] such as education, healthcare, or politics, and she notes that these norms "define and sustain essential activities and key relationships and interests, protect people and groups against harm, and balance the distribution of power."[66] Nissenbaum points out that "information technologies alarm us when they flout these informational norms,"[67] or rather, when they violate what she calls "contextual integrity." This justifies a good deal of the popular discomfort regarding the meteoric rise of Big Tech in recent years, which has drastically shifted social power dynamics, and it pinpoints the source of discomfort created by tech gothic novels like *New Waves, Little Brother,* and *The Circle,* in which a single, technological entity is given too much control over a particular tradeoff and skews it dramatically in a particular direction. For instance, the idea that discomfort stems from a violation of traditional social norms explains some of Mae's discomfort during the LuvLuv demonstration in *The Circle*; as demonstrated earlier, LuvLuv dramatically changes the social norms that most people abide by when getting to know one another, and this is precisely what makes Mae uncomfortable. Therefore, in order to make users more comfortable while still providing the notable benefits that can be achieved by

[65] Helen Fay Nissenbaum. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. (Stanford, Calif.: Stanford Law Books, 2010), 2.
[66] Ibid, 3.
[67] Ibid.

collecting and analyzing data, aiming to preserve context-relative informational norms would make more sense than striving to achieve complete privacy.

There has been some work within computer science to formalize the descriptive component of Nissenbaum's framework of contextual integrity; researchers have, for example, translated HIPAA into first-order temporal logic by defining syntax to express communication actions, the classification of roles that various individuals might play in a given context, and the state of an individual's knowledge:[68]

$$\text{inrole}(p_1, \textit{covered-entity}) \wedge \text{inrole}(p_2, \textit{individual}) \wedge (q = p_2) \wedge (t \in \textit{phi}) \quad (2)$$

$$\text{inrole}(p_1, \textit{covered-entity}) \wedge \text{inrole}(p_2, \textit{provider}) \wedge \text{inrole}(q, \textit{patient}) \wedge (t \in \textit{phi}) \quad (3)$$

$$\text{inrole}(p_1, \textit{covered-entity}) \wedge \text{inrole}(p_2, \textit{individual}) \wedge (q = p_2) \wedge (t \in \textit{psychotherapy-notes}) \rightarrow \Diamond\exists p : P.\, \text{inrole}(p, \textit{psychiatrist}) \wedge \text{send}(p, p_1, \textit{approve-disclose-psychotherapy-notes}) \quad (4)$$

$$\text{inrole}(p_1, \textit{covered-entity}) \wedge \text{inrole}(p_2, \textit{individual}) \wedge \text{inrole}(q, \textit{individual}) \wedge (t \in \textit{condition-and-location}) \wedge \Diamond\exists m' : M.\, \text{send}(p_2, p_1, m') \wedge \text{contains}(m', q, \textit{name}) \quad (5)$$

$$\text{inrole}(p_1, \textit{covered-entity}) \wedge \text{inrole}(p_2, \textit{clergy}) \wedge \text{inrole}(q, \textit{individual}) \wedge (t \in \textit{directory-information}) \quad (6)$$

Figure 2. Norms of Transmission from the HIPAA Privacy Rule

This type of formalization allows researchers to discover limitations of the specificity of the law and helps engineers by translating laws into succinct sets of logical requirements. Therefore, Nissenbaum's framework helps not only in "drawing the line" and defining the explicit boundaries of user privacy, but the work done on formalizing Nissenbaum's framework also helps to make this line concrete and implementable for developers and researchers.

However, there is one notable obstacle in that it is rather difficult to articulate exactly what current social norms are. Some computer scientists have made attempts to extract social

[68] Adam Barth, Anupam Datta, John C. Mitchell, and Helen Nissenbaum,"Privacy and Contextual Integrity: Framework and Applications," In 2006 IEEE Symposium on Security and Privacy.

norms by scraping and analyzing news and social media; for instance, researchers applied descriptive stats and sentiment analysis to a corpus of news on the web about the Facebook-Cambridge Analytica data scandal, and they were able to construct norms like "Permission from FB [transmission principle] to harvest profiles [attribute] in large quantities was specifically restricted to academic use [context]."[69] But as Jameson notes in "Progress versus Utopia," the present is "numb, habituated, empty of affect," and "inaccessible directly."[70] In other words, since people are habituated and desensitized to current social norms, these norms are difficult to perceive for what they truly are, and defamiliarization becomes necessary to expose the norms and unspoken rules that society operates under. Defamiliarization occurs under circumstances that have drastically changed, which implies that there are only two sources from which we can derive current norms: great turmoil and change (when there are new technological innovations, crises, or scandals) and speculative fiction. Therefore, contemporary speculative fiction is a crucial component in identifying the norms that must be preserved in Nissenbaum's framework of contextual integrity.

Conclusion

Little Brother, *New Waves*, and *The Circle* are all examples of tech gothic literature, and by drawing on traditional gothic motifs translated into their technological equivalents, they expose underlying privacy tradeoffs that society faces and demonstrate the consequences of handling these tradeoffs poorly. Every approach has its own benefits and failures, but ultimately, the line must be drawn somewhere. It is entirely possible that we will never find a compromise,

[69] "Applications of Contextual Integrity – Report from the 3rd Symposium," Tech Policy, accessed March 7, 2022, https://www.techpolicy.com/Report-from-3rd-Symposium-on-Applications-of-Contextual-Integrity_TH-012822, 12.
[70] Jameson, *Archaeologies of the Future*, 287.

and any line that we manage to draw will constantly shift with changes in public opinion and circumstance, but it is imperative that we at least try. Nissenbaum's work suggests how we might begin that task, while tech gothic novels reveal the perils of failing to do so.

Conclusion

This thesis examined previous conceptions of privacy, from the perspective of consumers, lawmakers, and computer scientists. Using Foucault's theory of authorship, however, allows for a more expansive definition of privacy as a form of authorship that allows users to control the representations of themselves through their data. This understanding of privacy helps to expose privacy violations in speculative fiction, which plays an important role as "edge cases" that reveal flaws in our existing societal framework. As novels of the tech gothic genre and privacy scandals that have occurred in recent years indicate, there are tradeoffs that society must face in preserving privacy, and the process of determining the appropriate threshold will involve compromise and an examination of traditional social norms.

In the past, introducing myself as a Computer Science and English joint concentrator has almost always prompted raised eyebrows and confusion. Many have pointed out that the two fields seem very different from each other, and they often claim that STEM is analytical while the humanities are creative. And yet, I have always believed that the two were not so different; one must be creative to find elegant solutions in computer science and analytical to craft a persuasive argument, after all. I've attempted to use this thesis to demonstrate how ways of thinking from CS and English can complement each other.

Writing this joint thesis in Computer Science and English has been both extremely challenging and incredibly rewarding. Attempting to explore computer science and English topics in depth and writing about them in a way that is accessible for readers who do not have a background in both fields has been difficult; balancing the need for sufficient description without

either drastically oversimplifying or going completely overboard with technical details or literary theory took a lot of practice, feedback, and revision to figure out. Also, writing a multi-disciplinary thesis has required that I not only apply techniques from one field to another, but also push arguments in both disciplines simultaneously. I often went through phases in which I would fixate on one aspect or another, which meant I would sometimes have to retroactively revise a chapter to incorporate a completely new argument without undermining or detracting from what was already there.

On the other hand, writing this thesis has allowed me to read a good deal of new literary and computer science theory. Finding unexpected parallels between computer science and literary studies has been so satisfying; seeing the similarities between privacy and authorship and realizing that novels with hyperbolic plots are the edge cases of literature were both completely accidental revelations that resulted from conversations with my advisors and annotations left in the corners of notebooks. This has strengthened my belief that computer science and English are more alike than they seem and that the two areas of study can be incredibly productive when put in conversation with each other.

I hope that the literary work of this thesis will help to clarify long-standing issues in computer science. Hopefully, the new framework of privacy as authorship will encourage software developers and engineers to grant users more explicit control over their data. Furthermore, I hope that the work of this thesis sufficiently demonstrates that fiction is useful to computer science as not only a forecast of new technologies but also an important medium that reflects popular opinion and social attitudes. In the past, computer scientists have relied heavily on surveys and social media to analyze public opinion and to understand the perspective of the

everyday consumer; it is my hope that contemporary literature can be considered as a valuable source for computer science research as well in the future.

I would like to build upon this work in the future by devising a framework or metric to describe degrees of privacy, as defined by authorship. This would make our newfound definition quantifiable and much more useful for computer scientists as they set goals in the process of developing their products. It would also be fascinating to apply this framework to the inevitable privacy incidents of the future; I believe that conceptualizing privacy as a form of authorship might offer new perspectives that can hopefully shape and influence future conversations around privacy.

Acknowledgements

First and foremost, I would like to thank my advisors, Professor James Waldo, Professor Sarah Dimick, and Jocelyn Sears for all their detailed feedback, advice, support, and guidance. For all the weekends and afternoons lost to answering my emails and reading my sleep-deprived writing. They have made me a better writer and a more knowledgeable computer scientist. I am so incredibly grateful to have had them as advisors and mentors; this thesis would not have crossed the finish line without them, and I have learned so much from them in the past year.

I would also like to thank my reader, Professor Cynthia Dwork. She has been a huge inspiration, and without *The Circle* and contextual integrity, this thesis would not be the same.

I also owe a great deal of thanks to Tim Hua, who let me use his GDPR data request results, as well as Kevin Chen, for taking on the role of rubber duck and Uber Eats. Thank you as well to my wonderful friends who have had the kindness and patience to encourage me throughout this grueling process: Michael Zhu, Teagan Seltzer, Elbert Du, and Anthony Cui.

And last but not least, I would like to thank my amazing parents, who never raised a single eyebrow when it came to Computer Science and English. Thank you for believing in me from day one.

Bibliography

"Applications of Contextual Integrity – Report from the 3rd Symposium." Tech Policy. Accessed March 7, 2022. https://www.techpolicy.com/Report-from-3rd-Symposium-on-Applications-of-Contextual-Integrity_TH-012822.

"California Consumer Privacy Act (CCPA)." State of California - Department of Justice - Office of the Attorney General, January 27, 2022. https://oag.ca.gov/privacy/ccpa.

"California Proposition 24, Consumer Personal Information Law and Agency Initiative (2020)." Ballotpedia. Accessed March 6, 2022. https://ballotpedia.org/California_Proposition_24,_Consumer_Personal_Information_Law_and_Agency_Initiative_(2020).

"Health Information & Privacy." Centers for Disease Control and Prevention. Centers for Disease Control and Prevention, September 14, 2018. https://www.cdc.gov/phlp/publications/topic/healthinformationprivacy.html.

"Health Insurance Portability and Accountability Act of 1996 (HIPAA)." Centers for Disease Control and Prevention. Centers for Disease Control and Prevention, September 14, 2018. https://www.cdc.gov/phlp/publications/topic/hipaa.html#one.

Privacy Online: a Report to Congress. 1998. Washington, D.C.: The Commission.

"What Is GDPR, the EU's New Data Protection Law?" GDPR.eu, February 13, 2019. https://gdpr.eu/what-is-gdpr/.

"What Is the 'Reasonable Expectation of Privacy'?" Findlaw, July 17, 2017. https://www.findlaw.com/injury/torts-and-personal-injuries/what-is-the--reasonable-expectation-of-privacy--.html.

U.S. Const. amend. IV.

Abrams, M. H, and Geoffrey Galt Harpham. 2015. *A Glossary of Literary Terms*. Eleventh edition. Australia: Cengage Learning.

Auxier, Brooke, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar, and Erica Turner. "Americans and Privacy: Concerned, Confused and Feeling Lack of Control over Their Personal Information." Pew Research Center: Internet, Science & Tech. Pew Research Center, August 17, 2020. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

Barrett, Brian. “Apple Backs down on Its Controversial Photo-Scanning Plans.” Wired. Conde Nast, September 3, 2021. https://www.wired.com/story/apple-icloud-photo-scan-csam-pause-backlash/.

Barth, A, A Datta, J.C Mitchell, and H Nissenbaum. 2006. “Privacy and Contextual Integrity: Framework and Applications.” In 2006 IEEE Symposium on Security and Privacy (S&P'06), 15 pp.–198. IEEE. https://doi.org/10.1109/SP.2006.32.

Corrigan-Gibbbs, Henry. “Keeping Secrets,” Stanford Magazine , November 7, 2014. https://stanfordmag.medium.com/keeping-secrets-84a7697bf89f.

Desfontaines, Damien. “Why Differential Privacy Is Awesome.” Ted is writing things, July 30, 2018. https://desfontain.es/privacy/differential-privacy-awesomeness.html.

Doctorow, Cory. 2008. *Little Brother*. 1st ed. New York, NY: Tor Teen.

Dwork, Cynthia, and Aaron Roth. 2014. *The Algorithmic Foundations of Differential Privacy: Foundations and Trends in Theoretical Computer Science.* Vol. 9. Hanover, Massachusetts: now. https://doi.org/10.1561/0400000042.

Eggers, Dave. *The Circle: A Novel*. New York: Vintage Books, 2014.

Encryption Working Group. “Moving the Encryption Policy Conversation Forward.” Carnegie Endowment for International Peace, September 10, 2019. https://carnegieendowment.org/2019/09/10/moving-encryption-policy-conversation-forward-pub-79573.

Foucault, Michel, and Paul Rabinow. 1984. *The Foucault Reader*. 1st ed. New York: Pantheon Books.

Foucault, Michel. 2008. “"Panopticism" from "Discipline & Punish: The Birth of the Prison"." *Race/ethnicity: Multidisciplinary Global Contexts* 2 (1): 1–12.

Geer, Dan, 2015. “The Right to Be Unobserved” in *IEEE Security & Privacy*, vol. 13, no. 04, pg. 88. New York, NY: IEEE Computer Society.

Jameson, Fredric. 2005. *Archaeologies of the Future : the Desire Called Utopia and Other Science Fictions*. London ; New York: Verso.

Kerr, Orin S. 2012. “THE MOSAIC THEORY OF THE FOURTH AMENDMENT.” Michigan Law Review 111 (3): 311–54.

LeMenager, Stephanie. 2017. “Climate Change and the Struggle for Genre.” In *Anthropocene Reading: Literary History in Geologic Times*, 1:220–38. University Park, USA: Penn State University Press.

Lemon, Lee T, Marion J Reis, and Gary Saul Morson. 2012. *Russian Formalist Criticism*. Lincoln: Nebraska Paperback.

May, Tiffany, and Amy Chang Chien. "Game over: Chinese Company Deploys Facial Recognition to Limit Youths' Play." The New York Times. The New York Times, July 8, 2021. https://www.nytimes.com/2021/07/08/business/video-game-facial-recognition-tencent.html.

McLaughlin, Jenna. "New Court Filing Reveals Apple Faces 12 Other Requests to Break into Locked Iphones." The Intercept, February 23, 2016. https://theintercept.com/2016/02/23/new-court-filing-reveals-apple-faces-12-other-requests-to-break-into-locked-iphones/.

Newton, K. M. 1997. *Twentieth Century Literary Theory : a Reader*. 2nd ed. Basingstoke: New York: Macmillan ; St. Martin's Press.

Nguyen, Kevin. 2020. *New Waves: A Novel*. Random House Publishing Group.

Nissenbaum, Helen Fay. 2010. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, Calif.: Stanford Law Books.

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

Real World Crypto, "Real World Crypto conference 2020: session 4," YouTube video, 1:39:06, February 13, 2020, https://www.youtube.com/watch?v=_CpjIFh0Kis.

Safronova, Valeriya. "The Rise and Fall of Yik Yak, the Anonymous Messaging App." The New York Times. The New York Times, May 27, 2017. https://www.nytimes.com/2017/05/27/style/yik-yak-bullying-mary-washington.html.

Vint, Sherryl. 2016. "Dystopian Science Fiction and the Return of the Gothic." In *The Oxford History of the Novel in English: Volume 7: British and Irish Fiction Since 1940,* ed. Peter Boxall, and Bryan Cheyette. Oxford: Oxford University Press.

Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism : the Fight for a Human Future at the New Frontier of Power*. First edition. New York: PublicAffairs.