Redefining Power Structures Surrounding Healthcare and Data Privacy

The most misleading illusion the technology companies today can generate is the perception that their products come at no cost. What they claim may be partially true — simply accessing the Internet or creating a social media account usually has no monetary cost. Yet consumers pay far more than they believe they are; an exorbitant cost comes in the form of users' brains and bodies in a metaphysical way that transcends the material and monetary world and cannot even be quantified. Google searches come at no cost because the searchers often become searched themselves. Facebook and other social media accounts are often free because the product is not the platform, but the users themselves.

As the Internet further increases in ubiquity of access, the largely exploitative features of technology can no longer be regarded as trivial. Especially in the context of healthcare, technology can decide a life or death issue. Technology like our smartphones or smartwatches can not only track users' every movement and conversations, but also predict their future behavior and events in their lives. This paper will focus on its applications to healthcare, wherein technologies can make assumptions about individuals' health history and outcomes before we even notice. Doctors, nurses, and other healthcare workers are no longer the only ones in control of our health. Rather, extensive networks invisible to most store patient healthcare data, raising serious questions regarding the privacy of the information. Rather than comb through mounting files of paperwork about an individual, a simple search algorithm can cue up almost anything about a patient's health history, to be utilized to a company's advertising wants or "abused by a malicious insider" (Diaz and Gurses, 2012). Almost everyone covered under a major healthcare provider such as Kaiser or Sutter Health receives care through their online system, where patients both interact with their doctors, make appointments, receive test results, and much more. Those oblivious to the data collection subject themselves to an progressively exploitative framework — sensitive information and personal data can be sold for large profits and positive margins with no payment to the creators of the information themselves. The proliferation and collection of personal data and knowledge churns an overwhelming profit in an economic model known as surveillance capitalism. With increasing data exploitation and surveillance capitalism, networks built through grassroots community efforts demonstrate a promising approach to reclaiming the right to healthcare privacy.

Knowledge is Control

Privacy as a whole warrants a preface of knowledge, which it protects. The age-old saying declares that knowledge is power. Power provides control. As such, knowledge can mean predictive power over a consumer's actions, behaviors, and even thoughts — which, in turn, provides the means to control. Knowledge may never be fully defined — it requires a knowledge of knowledge itself, of which is limited through human understanding. So much is yet unknown about knowledge that ontology serves as the field of study surrounding the means of expressing and articulating knowledge (Srinivasan, 2018). For big technology companies, the basis of their profit is knowledge — the more they know about their consumers, the more they can target advertisements and other marketing schemes to influence their behavior. For instance, the popular game Pokemon Go created a mass experiment that essentially herded players through specific locations and provided guaranteed footfall for establishments who paid the game to feature their businesses as hotspots (Zuboff, 2019). Unsurprisingly, Google executive John Hanke incubated the game as its chief investor (Zuboff, 2019). In association with the classic framework between the state and the war machine, technology completely reshapes the two actors' interactions (Delueze and Guttari, 1986). With the advent of the Internet, the war machine no longer localizes and moves between individual bodies, but instead as an extension of the very body itself. In modern society, the war machine can be likened to big technology companies whose sole purpose is to exploit and extract. For them, physical territories and borderlines have been rendered useless to their efforts through accessible networks that do not require an existence in material space (Deleuze and Guttari, 1986).

Knowledge Applied to Healthcare

In the field of healthcare, knowledge revolves around science and patient data. In the Enlightenment era of the 17th and 18th centuries, science became increasingly popularized as universities, societies, and other academies emerged as centers for individuals to deepen their scientific knowledge (Srinivasan, 2018). At the time, however, the so-called "centers for public knowledge" limited access primarily to rich white males, who, not coincidentally, wielded the most power in society (Srinivasan, 2018). Today, science itself represents a local knowledge body conducted in different places, by different people of different backgrounds, that cannot be

fit into a one size fits all model. Scientific knowledge extends beyond its common associations with Western medicine, which can sometimes demonstrate apparent contradictions with healthcare knowledge generated by communities (Verran, 2002). The scientific method may provide general guidelines for how an experiment should be conducted and how results should be analyzed, but the limits of scientific exploration are endless. For instance, in prescribed burnings of the land in Australia, both the scientific knowledge of climate scientists and old clan leaders' knowledge of how to go about the process may be equally valid (Verran, 2002). In the scope of the medical field, knowledge is also limited to Western standards in the United States. Western medicine rarely incorporates the herbal medicine used so commonly in the East, regarding treatments such as acupuncture almost as an entirely different branch of study (Lam 2001). Furthermore, healthcare knowledge still exists within the sovereignty of the few. Doctors, with the jurisdiction for anything from prescribing potent medications to advising on lifestyle changes, undergo years of training in medical school and residency to attain such privileges. While doctors' expertise can prove essential for the general public, the rest of the general population, specifically those who do not regularly attend doctor's appointments, are left out of the loop. The definition of health, albeit primarily liminal and existing within a fluid jurisdiction, largely adheres to medical advice and parallels medical training. Especially in low-income communities and racial minority populations, however, there exists an inherent mistrust of the medical system and healthcare providers due to "continuous and repeated discrimination, racism, and harmful experiences" throughout history (Bogart et. al, 2019). As a result, they feel more hesitant to receive medical treatment and follow doctors' advice, from the COVID-19 vaccine, to following healthy lifestyles such as regularly exercising (Bogart et. al, 2019).

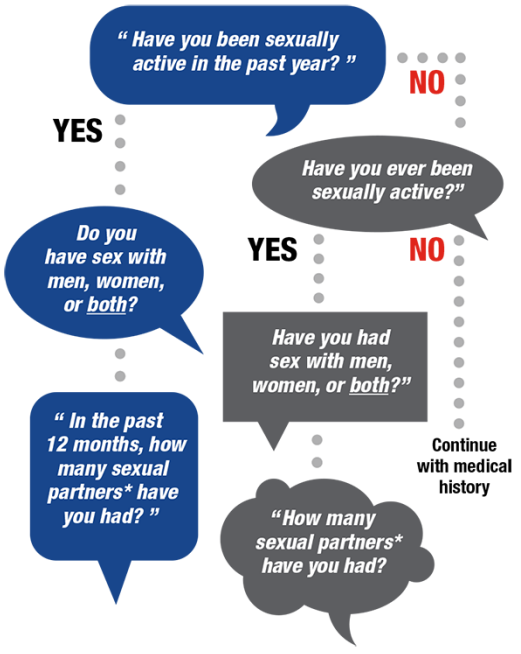
Introduction to Healthcare Privacy

The gravity of responsibility of knowing a patient's health history and habits, of having a patient confide in them, lends itself to the serious training doctors must undergo. The most uncomfortable moments of a doctor's visit may well be the answering of lifestyle-related screening questionnaires. The screeners ask personal questions that one's parents may not even want to be privy to — do you drink? If so, how much alcohol have you consumed in the past week? Do you have a history of sexual intercourse that could put you at risk of sexually transmitted diseases? Have you had adverse childhood experiences in the past? The number of

screeners about sensitive topics that can arise during doctor's visits are endless. Oftentimes, doctors may ask the patient directly during an appointment. Within the walls of a hospital room, and with patients given the option to have a parent leave, the conversations foster a sense of confidentiality between physician and patient. But what happens when computer networks can extend information past the confines of a building?

The increasing shift to online data collection over patients' health history, test results, and other data raises a longstanding ethical question about individual rights to privacy. When individuals share personal healthcare information with doctors, which later becomes stored in medical records and databases, who else should be able to access the information? Privacy hinges particularly on society and social norms. In the United States, the Health Insurance Portability and Accountability Act (HIPAA) of 1996 currently sets the guidelines for what can and cannot be shared about an individual (U.S. Department of Health & Human Services, 2000). In total, it lists 18 identifiers that are known as personal health information (PHI), such as names, Social Security numbers, and medical record numbers.

Online medical systems, although much more convenient and accessible to the common user, come with a dangerous sacrifice: privacy. What happens when private information becomes theoretically available to anyone who can bypass a system's security firewalls? What is the value of secrecy or privacy in a world where it seems to be gradually shrinking in significance? What does it mean to reclaim one's right to privacy, especially in regards to one's own body?



The Alcohol Use Disorders Identification Test: Interview Version

Read questions as written. Record answers carefully. Begin the AUDIT by saying "Now I am going to ask you some questions about your use of alcoholic beverages during this past year." Explain what is meant by "alcoholic beverages" by using local examples of beer, wine, vodka, etc. Code answers in terms of "standard drinks". Place the correct answer number in the box at the right.

1. How often do you have a drink containing alcohol?
(0) Never [Skip to Qs 9-10]
(1) Monthly or less
(2) 2 to 4 times a month
(3) 2 to 3 times a week
(4) 4 or more times a week

2. How many drinks containing alcohol do you have on a typical day when you are drinking?
(0) 1 or 2
(1) 3 or 4
(2) 5 or 6
(3) 7, 8, or 9
(4) 10 or more

3. How often do you have six or more drinks on one occasion?
(0) Never
(1) Less than monthly
(2) Monthly
(3) Weekly
(4) Daily or almost daily
Skip to Questions 9 and 10 if Total Score for Questions 2 and 3 = 0

4. How often during the last year have you found that you were not able to stop drinking once you had started?
(0) Never
(1) Less than monthly
(2) Monthly
(3) Weekly
(4) Daily or almost daily

5. How often during the last year have you failed to do what was normally expected from you because of drinking?
(0) Never
(1) Less than monthly
(2) Monthly
(3) Weekly
(4) Daily or almost daily

6. How often during the last year have you needed a first drink in the morning to get yourself going after a heavy drinking session?
(0) Never
(1) Less than monthly
(2) Monthly
(3) Weekly
(4) Daily or almost daily

7. How often during the last year have you had a feeling of guilt or remorse after drinking?
(0) Never
(1) Less than monthly
(2) Monthly
(3) Weekly
(4) Daily or almost daily

8. How often during the last year have you been unable to remember what happened the night before because you had been drinking?
(0) Never
(1) Less than monthly
(2) Monthly
(3) Weekly
(4) Daily or almost daily

9. Have you or someone else been injured as a result of your drinking?
(0) No
(2) Yes, but not in the last year
(4) Yes, during the last year

10. Has a relative or friend or a doctor or another health worker been concerned about your drinking or suggested you cut down?
(0) No
(2) Yes, but not in the last year
(4) Yes, during the last year

Record total of specific items here

Total scores of 8 or more are recommended as indicators of hazardous and harmful alcohol use. Higher scores indicate greater likelihood of hazardous and harmful drinking, or reflect greater severity of alcohol problems and dependence.

[1]A flowchart provided by the Center for Disease Control and Prevention that delineates how doctors can approach questions about sexual history (Center for Disease Control and Prevention, 2018)

[2] An example of the Alcohol Use Disorders Identification Test (AUDIT), a screener for alcohol disorders

The Importance of Privacy, Specifically in Relation to the Body

Technologies like the cellphone have become increasingly omnipresent in one's everyday life — for instance, a 2019 Pew Research Center study found that 96% of Americans own a cellphone of some kind (Pew Research Center, 2019). Due to their portable nature, cellphones and other technologies go wherever their owners go. As technology increasingly manifests as extensions of ourselves and our bodies, what it means to be human and what it means to be in control of our own bodies has simultaneously evolved (Deleuze and Guttari, 1986; Mbembe, 2017). Just as one's life story can be gleaned from "permanently available" social media profiles through a readily accessible Google search, so can one's biological makeup and function be predicted from one's online health profile (Solove, 2015). The tradeoff with social media tools, which "can simultaneously support grass-roots political mobilizations as well as government surveillance and human rights violations," applies to online healthcare tools as well (Coleman, 2010). The frequently heard calls for transparency pervade today's society, whether that be about politicians or big technology companies. They can be equated to "wars on secrecy," but little regard goes toward the implications of such endeavors (Mbembe, 2018). What becomes sacrificed when secrecy becomes abolished and transparency of the body becomes widely circulated? What power does that accord to those aiming to exploit and extract the very means of movement? When technologies can reveal our bodies in full transparency, it also exposes the very essence of who we are and the "truth of who we are" that is oftentimes "hidden inside our bodies" (Mbembe, 2018). The continual erasure of privacy concerning our bodies parallels the erase of distinction between humans and objects as technologies constitute more and more of our daily lives (Mbembe, 2017). While the blurring of borderlines between humans and objects can be regarded as almost emancipatory, there also exists a perennial devaluation of privacy, which may be worth more than millions to innovators of technology. Little would distinguish the traits of a human from mere descriptors that can also be applied to animate or inanimate objects. At the root of it, giving up privacy also means giving up the "liberal individual" who "could be the subject of democracy" (Mbembe, 2017).

The loss of democracy and declining privacy of our bodies lends itself to a serious "collective action problem" that nevertheless still has the potential to be reversed through law and democracy (Zuboff, 2019). Individual privacy is largely provided by societal norms, which dictate against intrusions such as peeking into a neighbor's window or into people's data files, as society recognizes that it would be "suffocating" without privacy protection (Solove, 2015). Hacking, especially of biometric and sensitive healthcare data, raises ethical questions when widely used in companies and government systems. When it comes to storing sensitive information such as health history and identifying information and taking extra privacy measures, however, only HIPAA holds against doing so. Societal norms value the appearance of privacy in spite of technologies increasingly threatening the status quo, adhering to how "the law should protect privacy not because we expect it, but because we desire it" (Solove, 2015). When it comes to the hacking and mishandling of biometric data, the law should protect privacy beyond the surface because it is necessary.

What Privacy Does HIPAA Provide?

A combination of HIPAA and the 2009 Health Information Technology for Economic and Clinical Health Act (HITECH) attempts to protect personal healthcare information from organizations that can capitalize on the data for marketing or other purposes (Burde, 2011). Combined, they stipulate regulations on what health providers and health insurance companies can share to other organizations. HITECH expands upon HIPAA in the realm of sharing electronic PHI (ePHI), extending HIPAA's restrictions to businesses in partnership with healthcare-related companies or providers (Burde, 2011). In addition to physical safeguards of patient data, healthcare entities must also create technical safeguards such as firewalls and encryption to protect electronically stored data. Under HITECH, patients requesting access to their data must be granted access within thirty days (Burde, 2011). The primary purpose of the HITECH Act, however, was to persuade healthcare providers to transition to ePHI recordkeeping to "improve the quality and efficiency of care delivered" (Adler-Milstein and Jha, 2017). As a result, hospitals adopted electronic health records at an almost 15% annually, a staggering increase from 3.2% before the passage of the act (Adler-Milstein and Jha, 2017).

Even though the HITECH Act reinforces previously lax HIPAA compliance with penalties that can go up to $1.5 million in total, businesses can still find ways to fly under the

radar (Burde, 2011). Nevertheless, the Human and Health Services seems to be moving toward incentives over punishments — a recent amendment to the HITECH Act, passed in January 2021, will award brownie points to businesses in compliance with HIPAA regulations (Hartsfield, 2021).

When Data Storage and Systems Go Wrong

What HIPAA and its amendments cannot protect, however, are the several loopholes around it and calamitous instances of cyberattacks. When privacy becomes violated, and knowledge rests in the wrong hands, healthcare systems can be severely compromised. Specifically when hospitals and other clinics rely on online databases to operate and store patient data, they become extremely vulnerable when criminal activity interferes with their systems (RSI Security, 2020). It is no longer localized to one or a few facilities, but a vast network of interconnected healthcare facilities across the globe. For instance, Universal Health Services found themselves the victims of a ransomware attack worth $67 million in losses in September 2020 (Lyngaas, 2021). Scrambling to take back the reins of their system, their information technology employees were forced to reroute ambulances to competitor hospitals and delay patient billing and other information for a few months (Lyngaas, 2021). Although no system, computer or physical, can be completely defensible, it is alarming that one of the largest healthcare providers so easily lost control of its computer networks. With the data breach, not only did the health network lose much of its revenue, but also it leaked treasure troves of data to the hackers responsible. The Universal Health Services attack represents just one out of many that have already transpired and that will transpire in the future. While robberies of physical files likely occurred just as often as did electronic stealing of information, the large scale databases can be extracted in a matter of seconds (RSI Security, 2020). Society's collective behavior will tell which side will ultimately win out in the security race against those enforcing security and those looking to crack it.

Approaching Privacy Protection

Objects, all subject to the natural laws of entropy, inevitably break and wear down over time. With material foundations, Internet technology also constitutes objects that gradually wear down physically (Srinivasan and Bloom, 2020). Code can break, malfunction, and fail to run. In

the framework of cyberattacks, code can be manipulated and heavily exploited. Devices such as smartphones, laptops, and tablets can be easily shattered into glass pieces in a moment of ineptitude. In order to approach digital healthcare privacy through the lens of law and societal norms, broken world thinking must be first considered (Jackson, 2014). The HITECH Act embodies broken world thinking — focused on dissolution and change instead of outright innovation, it allows healthcare providers to adapt previously paper-based files onto a digital network without having to create new files themselves. Electronic health records live in a constant state of repair, addition, and repurposing as patient healthcare metrics evolve and become updated (Jackson, 2014).

An appropriate repurposing of a famous quote from Leo Tolstoy's *Anna Karenina* addresses the ever present risk of data breaches in such electronic healthcare systems: ""'All working technologies are alike. All broken technologies are broken in their own way" (Jackson, 2014). Just as no "perfect human being or family" exists, objectively speaking, no "perfect technology" exists. Therefore, all existent technologies, especially electronic healthcare systems, represent the latter of Tolstoy's preface into the classic novel.

The Pitfalls of Imperialistic Thinking

Non healthcare-related issues of privacy that relate to technology in general cloud over issues specific to the healthcare sector. The capitalistic and exploitative frameworks that many companies must first be prefaced by discussing imperialist attitudes upon which they hinge and severely jeopardize user privacy. Religious parallels are often drawn to technology, likening the Internet to a God or Savior of sorts (Srinivasan and Bloom, 2020). When European colonists arrived in Africa on missionary trips to spread the gospel of Christianity, they invoked religion as the primary driving factor for their actions. Yet in addition to preaching about their Savior in Jesus Christ, they also largely assumed a savior complex. The viewpoint of the colonized population as inferior can now be dubbed imperialistic thinking, wherein the humanity of communities is neglected and the main modes of interaction involve extraction and exploitation of labor, data, and much more (Crawford and Joler, 2018). The same perspective endures today, wherein society looks well upon those who donate to developing countries or work directly with poorer countries. For instance, Google's new Artificial Intelligence (AI) lab in Accra, Ghana aims to bring groundbreaking innovations rooted in the continent of Africa itself (Srinivasan,

2019). While the actual effects of the lab lie in a gray area between beneficial and harmful, other major corporations such as Uber only take profit and customers away from local community businesses, such as the matatu minivan services (Srinivasan, 2019). More times than not, introducing new technologies to developing countries can harm the population more than help — the term "pilotitis" was specifically coined for new technologies that failed past the pilot phase (Srinivasan, 2019). Even if approached with non-imperialistic intentions, "sending aid is not always a panacea" (Srinivassan, 2019).

Ron Eglash, a professor in the School of Information at the University of Michigan, demonstrates the slippery slope of imperialistic thinking through his study of African fractals. Albeit having studied the subject for several years, Eglash's work seems to simplify the essence of African culture with a mathematical and algorithmic metaphor. The humanity etched into the "diversity of African cultures" becomes transformed into robotic and objective forms of data collection instead (Eglash 2007). While Eglash only goes so far to view African communities through the lens of data and algorithms, others directly affect disadvantaged populations through aid-based programs or organizations. For instance, the One Child Per Laptop (OCPL) project aims to execute exactly what the organization's namesake delineates: provide access to a laptop per child for lower income countries (Philip et. al, 2010). By selling low cost laptops at a wholesale price to developing countries and promising a one-to-one model for its donors, OCPL ultimately serves to contribute better technological resources under the philosophy that a "laptop can turn the lives of these children around" (Philip et. al, 2010). Although noble in its initial mission, the undertones apparent in one of OCPL's advertisements tells another story. In a chilling video, the organization contrasts the images of "Asian and African children hunched in manual labor" and "an African boy dressed shooting an automatic firearm" with "African boys wearing collared shirts engrossed in the iconically green XO laptop" (Philip et. al, 2010). In a mere thirty seconds, the video encapsulates several tropes and negative stereotypes associated with children from lower income countries. Through the visuals displayed on screen, the OCPL presents the laptop as an all-encompassing savior, just as religious missionaries proclaimed when colonizing their ancestors (Philip et. al, 2010). The OCPL broadcasts the message that kids need "the right tools" to thrive and grow in a positive environment, but disregards a crucial part of the journey in getting there. Supplying someone a computer is rendered useless unless they actually understand how to use the device itself, and the OCPL ultimately failed to address how children

can take advantage of the new age of "postcolonial computing" to truly effect the "end of colonialism" and the "end of exploitation" (Philip et. al, 2010). It is unsurprising that a few years after its initial launch, the project failed to both bolster students' learning in the classroom, as well as turn its laptop and other products into a cost-effective endeavor (Robertson, 2018).

The same parallels can be drawn to solutions surrounding healthcare privacy, wherein imperialistic thinking can alleviate surface level issues in the short-term, but ultimately leave the communities "served" in worse shape than before in the long-run. It may not be enough to administer healthcare services and collect patient data and research with populations starved of regular healthcare treatment, but rather impress a more sustainable model of care that the local community can implement itself (Skinner, 2019). It is not enough to simply make assumptions, but rather becoming immersed in the community allows technology innovators and service deliveries to analyze the needs of the community (Skinner, 2019).

Shifting the Focus to Local Efforts: Case Study of the Mexican Healthcare System

Several examples of community-based technological networks demonstrate that they are often the best solutions toward erasing the growing digital divide. As healthcare moves increasingly digital, from telemedicine to online appointment systems, technologies adapted by local communities may prove necessary toward improving the quality of care and preservation of privacy and PHI. Instead of approaching from an imperialistic point of view, those working directly with communities developing technologies need to first understand the complexities of the interactions at play — both the assemblage as a whole and within its individual parts.

Neighboring the United States directly to the south, Mexico's healthcare system exemplifies the necessity of comprehending the ins and outs of its structure. Under current president Andrés Manuel López Obrador (AMLO), the country transitioned to a centralized healthcare system and eliminated the 2003 Seguro Popular reforms previously in place (Reich, 2020). Previous criticisms of Seguro Popular can be summed up in AMLO's quote: "ni es seguro, ni es popular." Despite promising universal coverage of both the population and of services, Seguro Popular delivered neither, instead resulting in several out-of-pocket expenses and widespread corruption (Reich 2020). On the other hand, INSABI does not require a registration system or any out-of-pocket expenses for the services and supplies covered. However, INSABI does not provide as many services as Seguro Popular did, and more specific

procedures or services such as surgeries, chemotherapy, and dialysis would have to be paid fully out-of-pocket (Vallejo, 2020).

The implications of switching to INSABI are far-reaching for rural or poorer communities historically denied adequate access to healthcare and proper treatment. Several barriers to healthcare access exist in lower income communities, and INSABI both helps and harms them. While all Mexican citizens would be covered at no extra cost, those suffering from chronic diseases such as cancer and kidney failure will have to pay out-of-pocket to receive proper treatment (Vallejo, 2020).

Given the recent COVID-19 pandemic, Mexico has followed suit from other first world countries and shifted its health services online toward telemedicine efforts under the INSABI framework. Since many from local rural communities in Mexico cannot afford transportation to and from medical facilities, especially as they are often at least 60-90 minutes away, the INSABI network provides coverage for them online (Vallejo, 2020). Telemedicine provides access to those without transportation and therefore offers a promising alternative to healthcare treatment. For those with chronic illnesses, they may be essential to saving both money and time from frequent hospital visits. Nevertheless, Latin America as a whole has a lack of regulation on telemedicine and other digital technologies as compared to the United States. Mexico is only one of two countries with an "independent national data protection authority" — its version of HIPAA involves the General Health Law and regulations on other medicine-related supplies and services (Guerrero and Beach, 2020). However, the government exacts no regulations over software within digital apps. As a result, features such as location tracking or monitoring real-time information about a user or patient on the app are not subject to any consent requirements or regulatory approval (Guerrero and Beach, 2020). The question surrounding privacy resurfaces: what does privacy cost and what does it mean in an unregulated digital age?

Reclaiming Technologies from Larger Corporations

Recent grassroots efforts, especially among indigenous communities, to restore and reinvent technologies to cater to local populations exemplify a solution that strays away from relying on larger technology. A local community in Oaxaca, for instance, built an entirely community-based media framework (Srinivasan, 2019). In Australia, a consortium of five Aboriginal communities collaborated to develop the Outback Digital Network in 1998, also

known as the Tanami Network (Sawhney and Suri, 2008). The network consists of multiple projects, all of which serve to connect the communities together — for instance, the First Voices project preserves each tribe's language in digital format, while the Storyscape project promotes storytelling via audio and videoscapes (Sawhney and Suri, 2008). Created entirely separate from mainstream technologies, these networks are not subject to the privacy concerns that major search engines such as Google impose on their users. There stands no substantial barriers toward repurposing or expanding the technologies to better healthcare treatment for the communities as well. Indigenous communities in the United States, as well as other disadvantaged populations, can follow the example of the Tanami Network and the one established in Oaxaca to reclaim their own healthcare treatment from the status quo shown to them by larger healthcare providers and companies. Despite losing centrality of streamlined databases with a more far-reaching healthcare system, the localization of networks has the advantage of being less vulnerable to large-scale data breaches. In fact, doing so may begin to rebuild a trust so irretrievably broken from Hispanic or Black communities historically mistreated and undermined by the American medical system (Bogart et. al, 2019).

Conclusion

Privacy surrounds the accumulation of knowledge about an individual; knowledge means control. The gradual lack of privacy from technology-based corporations and organizations, especially in healthcare, has dangerous implications for the future. While much about healthcare technologies can be met with startling optimism regarding privacy, much can also evoke extreme cynicism. Nevertheless, the emergence of practices such as telemedicine and storing health data online is still relatively new, having been popularized only within the last ten years. Even the birth of the Internet itself is less than 100 years old. Surveillance capitalism, coined by Harvard Professor Shoshanna Zuboff as the increasingly capitalistic exploitation of privacy, is "barely 20 years old in the making, but democracy is old" (Zuboff, 2020). With novelty comes malleability and the flexibility to evolve and improve for the better. Transparency should not be seen as the be all and end all, but rather a privilege that those with access should tread carefully on. Privacy, on the other hand, should be treated as a right instead of a privilege. Despite its limitations, the HITECH Act exemplifies a promising starting point for laws surrounding the management of digital healthcare information in the United States and other countries like Mexico. Ultimately,

studies of local networks provide the best framework for recovering the right to privacy and confidentiality in the realm of healthcare, especially to disadvantaged populations who have been exploited the most. To do so, however, requires a thorough understanding of how local communities function and interact in the first place and a dismissal of imperialist attitudes when formulating solutions.

References

1. *Health Information Privacy. (2021, April 6). HHS.Gov. https://www.hhs.gov/hipaa/index.html*
2. *What Does the HITECH Act Do?* (2020, February 14). RSI Security. https://blog.rsisecurity.com/what-does-the-hitech-act-do/
3. Adler-Milstein, J., & Jha, A. K. (2017). HITECH Act Drove Large Gains In Hospital Electronic Health Record Adoption. *Health Affairs*, *36*(8), 1416–1422. https://doi.org/10.1377/hlthaff.2016.1651
4. Bogart, L. M., Dong, L., Gandhi, P., Ryan, S., Smith T. L., Klein, D.J., Fuller, L., & Ojikutu, B.O. (2021, March 1). *Vaccine Hesitancy Is High Among Black Americans, Including Health Care Workers*. RAND Corporation. https://www.rand.org/pubs/research_reports/RRA1110-1.html
5. Burde, H. (2011). THE HITECH ACT—An Overview. *AMA Journal of Ethics*, *13*(3), 172–175. https://doi.org/10.1001/virtualmentor.2011.13.3.hlaw1-1103
6. Coleman, E. G. (2010). Ethnographic Approaches to Digital Media. *Annual Review of Anthropology*, *39*(1), 487–505. https://doi.org/10.1146/annurev.anthro.012809.104945
7. Crawford, K., & Joler, V. (2018). Anatomy of an AI System. *Virtual Creativity*, 9(1). https://doi.org/10.1386/vcr_00008_7
8. Deleuze, G., Guattari, F., & Massumi, B. (1986). *Nomadology: The War Machine*. Semiotext(e).
9. Diaz, C., & Gurses, S. (2012). Understanding the landscape of privacy technologies. *Information Security Summit*, 1–6. https://www.esat.kuleuven.be/cosic/publications/article-2215.pdf
10. Guerrero, M. G., & Beach, A. (2020, December 14). *DIGITAL HEALTH APPS AND TELEMEDICINE IN MEXICO*. CMS.

https://cms.law/en/int/expert-guides/cms-expert-guide-to-digital-health-apps-and-telemedicine/mexico

11. Hartsfield, S. B. (2021, January 6). *HITECH Act Amended to Give Businesses Brownie Points for Certain HIPAA Security Programs*. Lexology. https://www.lexology.com/library/detail.aspx?g=77245ec6-39d9-4fbb-b995-aad1631aeb43
12. Jackson, S. J. (2014). Rethinking Repair. *Media Technologies*, 221–240. https://doi.org/10.7551/mitpress/9780262525374.003.0011
13. Lam TP. Strengths and weaknesses of traditional Chinese medicine and Western medicine in the eyes of some Hong Kong Chinese. Journal of Epidemiology & Community Health 2001;55:762-765.
14. Lyngaas, S. (2021, March 10). *Universal Health Services reports $67 million in losses after apparent ransomware attack*. CyberScoop. https://www.cyberscoop.com/universal-health-services-ransomware-cost-ryuk/
15. Mbembe, A. (2017, January 6). *The digital age erases the divide between humans and objects*. The Mail & Guardian. https://mg.co.za/article/2017-01-06-00-the-digital-age-erases-the-divide-between-humans-and-objects/
16. Universität Augsburg. (2018, November 26). *"Borders in a World of Networks: Who Can Move, Who Can't and Why?" - Achille Mbembe* [Video]. YouTube. https://www.youtube.com/watch?v=T1HniqDr_AU
17. Philip, K., Irani, L., & Dourish, P. (2010). Postcolonial Computing. *Science, Technology, & Human Values*, *37*(1), 3–29. https://doi.org/10.1177/0162243910389594
18. Reich, M. R. (2020). Restructuring Health Reform, Mexican Style. *Health Systems & Reform*, *6*(1), e1763114. https://doi.org/10.1080/23288604.2020.1763114
19. Robertson, A. (2018, April 16). *OLPC's $100 laptop was going to change the world — then it all went wrong*. The Verge. https://www.theverge.com/2018/4/16/17233946/olpcs-100-laptop-education-where-is-it-now
20. Sawhney, H., & Suri, V. R. (2008). Lateral Connectivity at the Margins. *Science, Technology and Society*, *13*(2), 345–368. https://doi.org/10.1177/097172180801300209

21. Skinner, D., Franz, B., & Kelleher, K. (2019). How Should Health Care Organizations and Communities Work Together to Improve Neighborhood Conditions? *AMA Journal of Ethics*, *21*(3), E281-287. https://doi.org/10.1001/amajethics.2019.281
22. Solove, D., Roessler, B., & Mokrosinska, D.(2015). *Social Dimensions of Privacy: Interdisciplinary Perspectives (Cambridge Intellectual Property and Information Law)*. Cambridge University Press.
23. Srinivasan, R. (2018b). *Whose Global Village?: Rethinking How Technology Shapes Our World* (Reprint ed.). NYU Press.
24. Srinivasan, R., & Bloom, P. (2020, June 30). *Tech barons dream of a better world — without the rest of us*. Salon. https://www.salon.com/2020/06/30/tech-barons-dream-of-a-better-world--without-the-rest-of-us/
25. Vallejo, O. M. (2020, March 27). *Salud pública en México: un paralelismo entre el INSABI y el Seguro Popular*. CEPLAN. https://ceplan.com.mx/salud-publica-en-mexico-un-paralelismo-entre-el-insabi-y-el-seguro-popular/
26. Verran, H. (2002). A Postcolonial Moment in Science Studies: Alternative Firing Regimes of Environmental Scientists and Aboriginal Landowners. *Social Studies of Science*, *32*(5), 729–762. https://doi.org/10.1177/030631202128967398
27. Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Illustrated ed.). PublicAffairs.
28. Zuboff, S. (2020, January 25). *Opinion | You Are Now Remotely Controlled*. The New York Times. https://www.nytimes.com/2020/01/24/opinion/sunday/surveillance-capitalism.html