PROTECTING HEALTH DATA WHERE CURRENT LEGISLATIONS FALL SHORT

A Research Paper submitted to the Department of Engineering and Society
In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science in Systems Engineering

By

Darby Anderson

March 27, 2020

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

ADVISOR
Catherine D. Baritaud, Department of Engineering and Society

Mobile health (mHealth) and electronic health (eHealth) interventions serve increasingly important roles as substitutions and additional aides to healthcare services. A lack of professionals, high cost of service, inadequate insurance coverage, insufficient desire, and mistrust of doctors contribute to the usage of mHealth and eHealth services (Harvey & Gumport, 2015). Some insurance companies provide these tools for their clients, while some interventions are provided by independent businesses, research groups, or citizen researchers. These products vary in both their usage and platforms, such as mobile applications, wearable devices, and online websites. Many mHealth and eHealth platforms, however, focus on individual characteristics and demographics for specific treatments (Grady et al., 2018). Although most health professionals practice this specialized type of treatment, the use in an online setting raises concern regarding the handling of such private information. Additionally, the widespread prevalence and easy access of these technologies, i.e. the more than 325,000 health and fitness mobile applications available on the market in 2018, allows anyone to become a "patient" (Young, 2018). Since anyone can download and begin using the platform without supervision or recommendation, it becomes complicated whether the user should be considered a patient or merely a consumer. An excellent example of this new frontier is a new mental health mobile application that seeks to reduce anxiety among users of the app. MindTrails, currently in use as an eHealth intervention, attempts to simultaneously treat users and collect data regarding the quality of the program in a study showcasing the benefits of a technique called cognitive bias modification-intervention (CBM-I). In this case, the user acts as a consumer of the application, patient of the treatment, and participant in the study. The options are endless for a consumer to find help as there exist over 10,000 mobile applications for mental health. Studies have also found that people with mental illness are willing to use their mobile phones to track and treat their mental health (Marshall,

Dunstant, & Bartik, 2019). However, most of the apps available lack a privacy policy or terms of agreement expressing data sharing to third parties and cannot guarantee the safety of the users' data (Robillard et al., 2019). A poll released earlier this year by America's Health Insurance Plans found that 62% of Americans value stronger privacy protections for their health information over easier access. The same poll shared that 90% of Americans believe that private technology firms should be held to the same standard as health care providers (America's Health Insurance Plans, 2020). The technology firms' rampant expansion on health applications most likely stems from the profitable industry of the health market and big data. Global Market Insights, Inc. predicts that the digital health market will grow globally to reach $504.4 billion by 2025 (Global Market Insights, 2019). Giant tech corporations like IBM, Google, and Microsoft have already tapped into the field by partnering with health organizations to get access to patient data in order to develop machine learning algorithms for treatments. Specifically, the partnership between Google and Ascension has ignited fear over data access and privacy between a healthcare provider and the second largest corporation in America (Rodrigo, 2019). Americans have just now begun questioning who has the right to access their personal health data and to what extent.

CURRENT STATUS OF LEGAL PROTECTIONS

In the U.S., the rights of its citizens are protected by legal documents. The Constitution in 1789 began this explicit declaration with many other bills following suit later expressing citizens' rights that may have not been specifically defined. Most of these legislations came to be as a result of some crisis that identified the lack of government protection for a citizen. Thus, for the most part, the government is considered to be more reactionary compared to proactive. This

characteristic has led to the creation of numerous statutes over the years aimed at protecting the rights of citizens. One very important right that has evolved over the years is the privacy of personal information. Although no singular amendment in the Bill of Rights expressly protects the privacy of personal information, many of them guard against certain privacies of a person. The Ninth Amendment attempts to cover any privacies not specifically mentioned by stating that the "enumeration of certain rights shall not be construed to deny or disparage other rights retained by the people" (Linder, 2019, para. 1). Federal legislations have been enacted over time to protect personal information from specific entities not covered or defined in previous acts. Figure 1 illustrates Chabinsky and Pittman's analysis of the numerous bills passed over time that protect the personal information of citizens against certain organizations (2019). The passing of the Federal Trade Commission Act in 1914 began the slow evolution of privacy acts. Not until almost 60 years after that did another important privacy law get passed: the Fair Credit Reporting Act (FCRA). It would take another thirty years

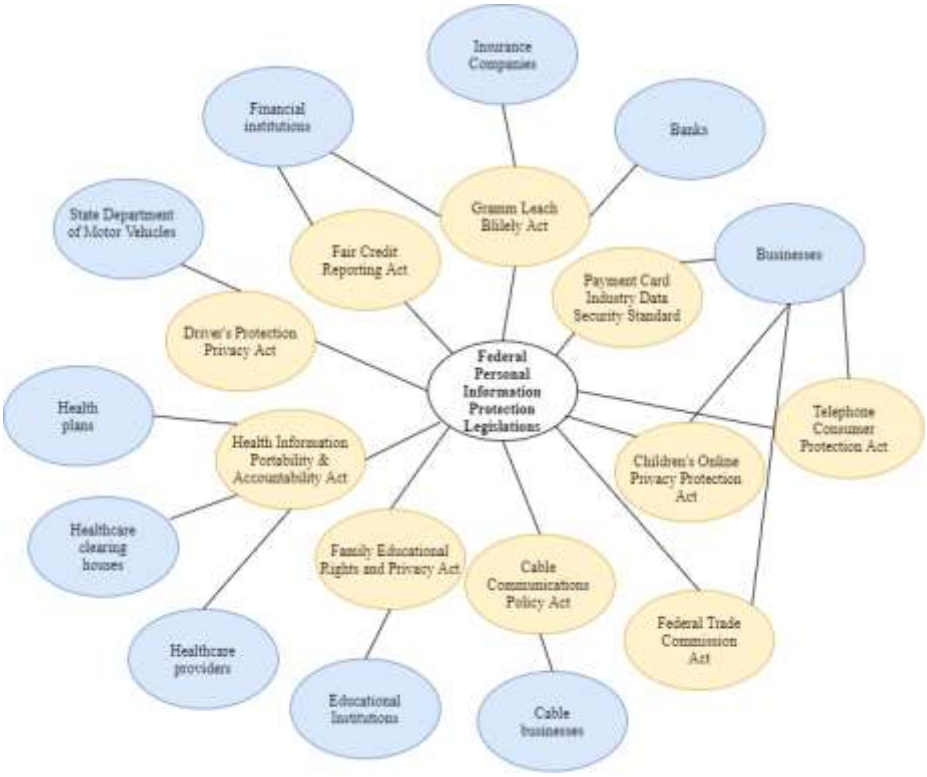

Figure 1: U.S. federal legislations designed to protect consumers: In the 20th century, many acts were created with the purpose of protecting certain rights of consumers, especially regarding personal information. Over time, some of these legislations have been revised to reflect more current use of technology (Anderson, 2020).

after the FCRA to create more privacy laws to protect citizens like the Telephone Consumer Protection Act in 1991, Driver's Protection Privacy Act in 1994, Health Insurance Portability and Accountability Act in 1996, and Gramm-Leach-Bliley Act in 1999 (Chabinsky & Pittman, 2019). The U.S. way of creating specific sector-based statutes to protect consumers from individual organizations displays the gaps created because of this reactionary way of thinking.

A major gap in the current U.S. framework lies in protecting health data. There is no act that specifically protects the ways in which businesses can use consumers' health data. Currently, an American citizen who has health insurance will have his or her health information protected when receiving treatment from a provider or hospital. Protection comes in three forms: Health Insurance Portability & Accountability Act (HIPAA) enacted in 1996, Federal Trade Commission (FTC), and state laws. HIPAA, a federal law which protects individual health information carried by entities, requires privacy and security minimums through their Privacy, Security, and Breach Notification Rules. The FTC protects consumers against malpractice and dishonest use of consumers' personal information used by businesses. Individual states have created laws that specify legal usage of personal data under certain business situations. For example, California adopts more stringent privacy laws that protect its residents. California's Consumer Privacy Act defines clear ways in how businesses can use Californians' data. However, this act only applies to businesses over a certain size and does not protect data considered to be covered under HIPAA (Chabinsky & Pittman, 2019). Thus, it may be easier to establish a federal law that targets missing entities and requires strict standards to cover all U.S. citizens. The Health Insurance Portability & Accountability Act only applies to entities including health plans, healthcare clearing houses, and healthcare providers. (U.S. Department of Health and Human Services [HSS], 2016). The Federal Trade Commission applies to

businesses but has a broader scope in its overall mission revolving around antitrust laws and consumer rights. Incorporating Actor Network Theory (ANT) to determine the key players involved in consumer health data, it can be seen that neither of these two acts can solely protect consumer health data against businesses. Actor Network Theory began in the 1980s by Callon, Latour, and Law (Rhodes, 2009). Its main premise incorporates players, either people or things, in a network and shows how they impact and interact with each other. A solution created from ANT would be a supported network that evolved from the old system, bringing in new players and different relationships (Rhodes, 2009). The visualization created below shows that the current infrastructure has failed in protecting consumer rights. Figure 2 below provides a digestible diagram of the current protection of consumer health data and rights by HIPAA and the FTC.

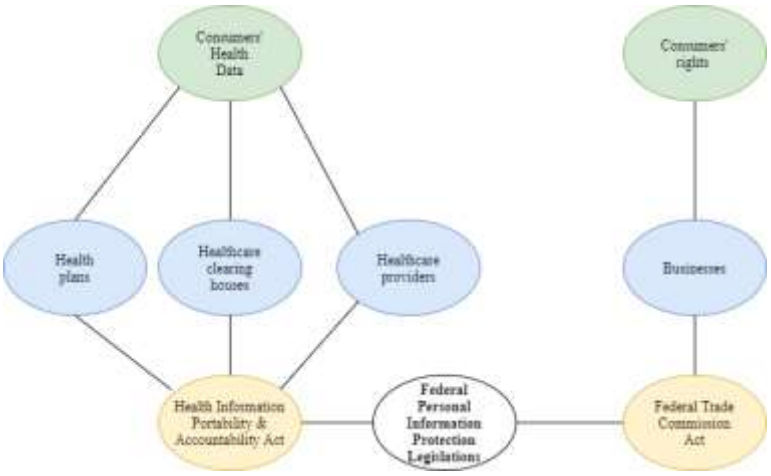

Figure 2: Current Actor Network Theory of protecting health data from businesses: At the center of the diagram remains federal legislations, which can be considered the only source of protection of consumers in the U.S. Two specific acts of this broader category include HIPAA and the FTC. However, it can be see that the covered entities of these statutes differ through what they safeguard (Anderson, 2020).

The lack of coverage raises the question on how the government can become proactive against future impediments on data privacy. One option that some experts in the field have advocated for regards the expansion of HIPAA to cover more entities. Nancy Davis, a director of compliance and safety at Door County Medical Center, a critical-access hospital in Door County, Wisconsin,

explains that she "would relish one set of laws. In a perfect world, HIPAA would be the end-all—not separate set of rules for minors or mental health" (Butler, 2017, "Gaps Between State and Federal Privacy Laws" section, para. 2; https://www.dcmedical.org/about). However, others, like Attorney Adam Greene, who specializes in health privacy law at Davis Wright Tremaine law firm in Washington, DC, "think[s] there's a danger in trying to extend HIPAA to other types of entities. HIPAA was designed very much with healthcare providers and health plans in mind. So just throwing a mobile app, a consumer-faced mobile app, into HIPAA is not necessarily the best fit" (Butler, 2017, "Some Say Supplement HIPAA, Don't Replace It" section, para. 2). The act's mission at the beginning was to provide a better way to transport medical data. It was only years after its creation in 1996 that several security measures were added to ensure the safety and privacy of data as more hospitals were transitioning to electronic health records. Thus, a more creative solution must be considered instead of revising an old policy to meet gaps previously unfulfilled.

TWO FEDERAL AGENCIES' ROLES IN SAFEGUARDING DATA

The U.S. Department of Health and Human Services (HSS) currently oversees the Health Insurance Portability and Accountability Act while the Federal Trade Commission's domain relates to business and consumer protection. A bipartisan federal agency, the FTC, balances the dual roles of protecting consumers while also promoting competition in the marketplace (https://www.ftc.gov/about-ftc/what-we-do). Although in nature the agency is bipartisan, the chair of the FTC, appointed by the President, can reflect different values compared to previous heads. Currently, the head of the FTC, appointed by President Donald Trump, is Joseph Simons. In this case, Joseph Simons has experience in antitrust, but not data protection (Kang, 2019).

Simons's, a Republican lawyer, main interest revolved around antitrust regulation prior to being elected as head of the commission. This lack of experience may not prepare him for the incoming responsibilities of the FTC. However, Simons explains that even the FTC act, created over 100 years ago, had no way of knowing the evolution of technology and the impending entrenchment on data privacy. For example, the FTC fined Google $22 million in 2012 for data privacy issues, and just recently the FTC imposed its biggest fine to date, $5 billion to Facebook (Fair, 2019). Big moves like this from the FTC creates precedence for other companies to double-check their actions and ensure they align with legislation to date. In addition to the fine, the FTC implemented new privacy rules for Facebook, including the establishment of an Independent Privacy Committee as well as designated compliance officers (Fair, 2019). A novel action like this also provides some inspiration for future deterrents for companies.

Meanwhile, the Department of Health and Human Services can only enforce its strict privacy and security rules through Health Information Technology for Economic and Clinical Health Act (HITECH) and the Privacy and Security Rule upon its covered entities. The HITECH update, added in 2009, strengthened the control of users over their data being marketed to third parties. The HIPAA Privacy Rule specifically protects the privacy of personal health information shared between covered entities and related parties. HIPAA's Security Rule, on the other hand, sets standards for encrypting and storing data for its covered entities (HSS, 2019). To ensure that these rules are met, the Office for Civil Rights (OCR) audits HIPAA entities. However, the small probability that an organization will become one of the 150 pulled by the OCR causes many entities to treat the rules of HIPAA as guidelines rather than serious laws (Butler, 2017). Additonally, HIPAA settlements do not pose too much of a threat to these very profitable organizations. In 2018, the largest settlement amounted to only $3.5 million, much smaller than

the 2019 $22 million fine to Google and $5 billion fine to Facebook (HIPAA Journal, 2019).Yet, even if these rules are continually met by the entities, the sensitivity of health data requires additional security measures and protections. Jordan Harrod, a Ph.D. student at a Harvard-MIT program, argued that the few updates throughout the years are insufficient. For example, she asserts that machine learning has been able to "de-crypt" the encryption standards set up by HIPAA. She cited a 2018 study which showed that machine learning could re-identify up to 95% of anonymous data when matched with another data source with the same individuals. These results prove meaningful as they show that publicly available information, like voting information, or private information, bought from a third party, can be used to match a person's anonymous health data (Harrod, 2019). Many users are unwillingly giving their information to third parties. These users may not realize the extent of HIPAA's protection when they assume it protects all types of medical data.

FINDING SYNERGY BETWEEN FTC AND HSS

Building a connection between the FTC and the HSS could prove beneficial as an alternative to updating HIPAA as both agencies provide different strengths in creating a solution for protecting consumer health data. For example, Patrick Austin for *Time* magazine comments that Google's recent acquisition of FitBit worries many about consumer health data (2019). The stated reason for the purchase, as explained by Google's Senior Vice President of Devices & Services Rick Osterloh, has to do with Google's expectations to shape wearable technology. Many speculate whether this acquisition was motivated by the access to the millions of consumer health data. FitBit, an independent hardware company that started 12 years ago, has slowly been collecting every possible type of health information on its users. It also has been making deals

with insurance companies and the wellness programs within corporations. Austin warns that these deals could become the stepping stones that Google needs to make it into the $24 billion health tech industry (2019). However, as stated before, HIPAA does not protect wearable devices' health data and providing a company who already has access to millions of consumer's data creates worry for both the FTC and the HSS.

The FTC's Take on Creating a Solution to Match the Evolution of Data Accessibility

In 2016, a report jointly written by the HSS and FTC was released acknowledging HIPAA's lack of coverage after the FTC first published a report on privacy and security in the "Internet of Things" ("IoT") (Federal Trade Commission [FTC], 2015). The FTC staff defines "IoT" as "the ability of everyday objects to connect to the Internet and to send and receive data" (FTC, 2015, "Executive Summary" section, para. 1). They explain which agencies have the jurisdiction to protect information created from new technology platforms. For example, the Fair Credit Reporting Act (FCRA), which establishes limits on the use of personal information for certain accreditations, would not cover companies that collect data from personal devices to make decisions regarding finance or insurance. It is therefore legal for an insurance company to accept wearable fitness tracker data from a client in exchange for lowering rates. The report also mentions Google and Microsoft's subsequent health platforms, "HealthKit" and Microsoft Health, respectively. Intel has plans for launching a platform that allows for the collection, storage, and analysis of health data. Thus, this pace of technological development creates pressure on lawmakers to define rules to match the current use of data. The FTC staff recommends several measures for companies to consider implementing. They revolve around data security, data minimization, and notice and choice. A first step to take for data security

regards the "security by design" and establishes design techniques that institute security into devices from the beginning. Additionally, product security should be maintained at every possible level of the organization, not just with the developers. Service providers should also be considered and ensure that servers exist at a certain level of security. Data accessibility needs to be monitored to require credentials to access information about consumers within or outside the company. A final recommendation on data security comes from the life cycle of the product and for companies to continuously monitor data and usage throughout its life. The Commission also offers data minimization as another important idea for companies to consider. Collecting vast amounts of data increases the vulnerability of both the data on the device and the cloud on which it can be stored. Taking every piece of information about a consumer also increases the chances of the data being misused in a way that misaligns with customers' desires. Defining scope and goals can help a company determine if the information collected helps only at this point in time or some time in the future. Sometimes future developments do not necessitate the collection of certain personal information. De-identifying the information also proves useful in collecting arrays of information. However, the FTC staff reminds the reader that many "de-identified" or anonymous information can be re-identified. Finally, the Commission concludes with incoporating the user among its recommendation. They believe that giving the user an option for consent would help with user expectations and desires. In a workshop conducted by the FTC, one participant expressed their concerns over fitness and health monitoring devices stating

> data from these Internet of Things devices should not be usable by insurers…Not should these data migrate into employment…credit…housing decisions…To aid the develop of the Internet of Things…we should reassure the public that their health data will not be used to draw unexpected inferences into economic decisionmaking (FTC, 2015, "Summary of Workshop Discussions" section, para. 3).

Overall, the FTC recommended that a new piece of legislation protecting data needs to be enacted, specifically one that is technology-neutral.

Protecting Personal Health Data Act Poses as Possible Solution

Minnesota Senator Amy Klobuchar and Arkansas Senator Lisa Murkowski propose a legislation that could fall in line with the FTC's recommendations. The Protecting Personal Health Data Act, already introduced into Congress, checks the requirement of being technology-neutral as it applies to the new health technologies not currently covered by laws. A key motivation of the act focuses on "help[ing] [to] strengthen privacy and security protections for consumers' personal health data" against business such as health apps, fitness trackers, and DNA kits (Klobuchar & Murkowski, 2019, p. 6). This bill, if passed, proves critical for users as many explain that the apps and digital trackers themselves are not the problem, but rather the privacy surrounding their data they submit and whether it would be "exposed, misused or exploited" (Harwell, 2019, para. 7).

The passing of this bill would include several provisions such as establishing security standards, consent requirements, de-identification standards, data minimizations, and a National Task Force. It can be understood that many of these provisions stemmed from the FTC's recommendation in their 2017 Staff Report. Specifics of such standards are not included in the bill, most likely due to the need of expert input to establish relevant requirements. One unique addition to the bill, not mentioned by the FTC, is the creation of a "Task Force". The Task Force on Health Data Protection would comprise of individuals with various backgrounds to "evaluate cybersecurity risks and privacy concerns" (Richardson, 2019, para 2). The duties would range from researching de-identification methods, security standards, and cybersecurity risks. In total,

15 members would comprise the group, and in one year's time they would submit a report with their recommendations (Klobuchar & Murkowski, 2019). Although the results of this bill, if passed, may not be immediately seen, its breadth of requirements as well as applicability to a range of consumer devices provides a stepping stone for the government to become more involved in companies' data handling processes. Figure 3 at the bottom illustrates how this bill, if passed, could draw a line between businesses and consumer health data. Using Actor Network Theory, essential connections can be realized among the various players and organizations within consumer data protection. With Actor Network Theory, its important to consider which actors could possibly be added to the network and how networks too can be changed. Federal legislations already play a major role in protecting data from various organizations. Incorporating the proposed solution merely adds another actor to the network, Protected Health Data Act, which will thus establish a new connection between businesses and consumer health data.

Protecting Personal Health Data Act's more narrow scope increases its chances of getting passed, although its specificity brings challenges. The bipartisan bill's quick time frame and specific guidelines could help Congress pass the bill, unlike attempts to revise HIPAA which could take years to agree upon and execute. However, in the bill, not all forms of health data are

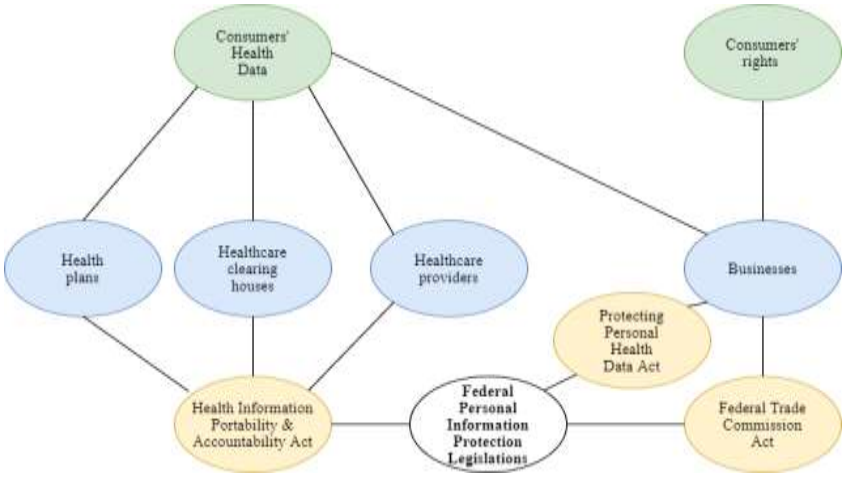

Figure 3: Updated Actor Network Theory of protecting health data from businesses: In the revised diagram, adding the Protecting Personal Health Data Act will target businesses in the specific involvement of personal health data. Instead of expanding the jurisdiction of HIPAA or broadening the responsibilities of the FTC, a bill can be passed to protect consumers' health data in the hands of businesses (Anderson, 2020).

protected. For example, if personal health data can be derived from other personal, although not health-related data, then the act would not apply. So, if an organization collects demographic data and uses it to determine health qualities, then that entity would be exluded. Furthermore, businesses that collect this data for "substantial" reasons may become exempt from the Task Force's jurisdiction. The vagueness of the word "substantial" could result in several meanings and exaggerated definitions (McGraw & Kuraitis, 2019).

WHAT THE FUTURE COULD LOOK LIKE IN THE HEALTHCARE TECH SPACE

To ensure that the effort made in protecting health data is worthwhile, it is important to look at the future to see the possibilities of changing technology. Seeing the exponential advancement of technology in the past, it's hard to imagine what our world will look like in the distant, or even not-so-distant future. Five healthcare companies were recently interviewed about their views on the state of the healthtech space in the next decade. Blink Health brought up mobile experience as a trend for digital health to give treatment and medication access to more individuals. Pager, another healthcare company, points to artifical intelligence and machine learning as catalysts to a major shift in health analytics. Pager's CEO, Walter Jin, explains that machine learning "will synthesize enormous and disparate data sources from electronic health records, wearables and social determinants of health into tangible, actionable insights" (Zitomer, 2019, "Pager" section, para. 3). Although this may seem like incredible prowess, this should concern individuals about healthcare companies taking advantage of their information and using it for "insights". The lack of knowledge about who has access to what causes most people to be unaware of the dangers in giving "disparate data sources" to one company. Zipari, a technology company that specializes in health insurance, also believes wearables and smart devices are key

in making insights, while Amplicare, another healthcare technology company, emphasizes personalization as the focus in the future (Zitomer, 2019). Either option would use sensitive personal data that most likely has not been used in the past. That is why it is critical now to establish stringent rules on the data that companies use to make economic or other decisions about a person. Most advancements in technology provide ease and comfort to a user, however, in this case, one wonders who is benefiting the most from the access to millions of data.

WORKS CITED

America's Health Insurance Plans. (2020, January). *Personal privacy outweighs increased transparency* [Press Release]. Retrieved from https://mms.businesswire.com/media/20200123005697/en/769272/1/202001-AHIP-MAPolling-FINAL.pdf?download=1

Anderson, D. (2020). *Current Actor Network Theory of protecting health data from businesses.* [Figure 2]. *STS Research Paper: Protecting Health Data Where Current Legislations Fall Short* (Unpublished undergraduate thesis). School of Engineering and Applied Science, University of Virginia. Charlottesville, VA.

Anderson, D. (2020). *Updated Actor Network Theory of protecting health data from businesses.* [Figure 3]. *STS Research Paper: Protecting Health Data Where Current Legislations Fall Short* (Unpublished undergraduate thesis). School of Engineering and Applied Science, University of Virginia. Charlottesville, VA.

Anderson, D. (2020). *U.S. federal legislations that protect consumers.* [Figure 1]. *STS Research Paper: Protecting Health Data Where Current Legislations Fall Short* (Unpublished undergraduate thesis). School of Engineering and Applied Science, University of Virginia. Charlottesville, VA.

Austin, P. (2019, November 4). The real reason Google is buying Fitbit. *Time.* Retrieved from https://time.com/5717726/google-fitbit/

Butler, M. (2017). Is HIPAA outdated? While coverage gaps and growing breaches raise industry concern, others argue HIPAA is still effective. *Journal of AHIMA, 88*(4), 14-17, 52. Retrieved from https://bok.ahima.org/

Chabinsky, S. & Pittman, F. (2019, March 7). *USA: Data protection 2019.* Retrieved from https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa

Fair, L. (2019, July 24). FTC's $5 billion Facebook settlement: Record-breaking and history-

making [Blog Post]. Retrieved from https://www.ftc.gov/news-events/blogs/business-blog/2019/07/ftcs-5-billion-facebook-settlement-record-breaking-history

Federal Trade Commission. (2015, January). *Internet of things: Privacy & security in a connected world.* Retrieved from https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

Global Market Insights, Inc. (2019, March 6). Worldwide digital health market to hit $504.4 billion by 2025: Global Markets Insights, Inc. *PR Newswire*. Retrieved from https://www.prnewswire.com/news-releases/worldwide-digital-health-market-to-hit-504-4-billion-by-2025-global-market-insights-inc-300807027.html

Grady, A., Young, S. Sutherland, R., Lee, H., Nathan N., & Wolfenden, L. (2018). Improving the public health impact of eHealth and mHealth interventions. Australian and New Zealand Journal of Public Health, *42*(2). doi.org/10.1111/1753-6405.12771.

Harrod, J. (2019, May 15) Health data privacy: Updating HIPAA to match today's technology challenges [Blog Post]. Retrieved from http://sitn.hms.harvard.edu/flash/2019/health-data-privacy/

Harvey, A. G., & Gumport, N. B. (2015). Evidence-based psychological treatments for mental disorders: Modifiable barriers to access and possible solutions. Behaviour research and therapy, *68*, 1-12.

Harwell, D. (2019, April 25). Code words and fake names: The low-tech ways women protect their privacy on pregnancy apps. *The Washington Post.* Retrieved from https://www.washingtonpost.com/technology/2019/04/25/code-words-fake-names-low-tech-ways-women-protect-their-privacy-pregnancy-apps/

HIPAA Journal. (2019, January 3). Summary of 2018 HIPAA fines and settlements [Blog Post]. Retrieved from https://www.hipaajournal.com/summary-2018-hipaa-fines-and-settlements/

Kang, C. (2019, March 8). The man deciding Facebook's fate. *The New York Times.* Retrieved from https://www.nytimes.com/2019/03/08/technology/ftc-facebook-joseph-simons.html

Klobuchar, A. & Murkowski, L. (2019). *Protecting personal health data act*. Retrieved from https://src.bna.com/I7O

Linder, D. (2019). The right to privacy [Blog Post]. Retrieved from http://law2.umkc.edu/faculty/projects/ftrials/conlaw/rightofprivacy.html

Marshall, J., Dunstan, D., & Bartik, W. (2019). The digital psychiatrist: In search of evidence-based apps for anxiety and depression. *Frontiers in Psychology, 10,* 831. doi:10.3389/fpsyt.2019.00831

McGraw, D, & Kuraitis, V. (2019, August 19). Protecting health data outside of HIPAA: Will the Protecting Personal Health Data Act tame the Wild West? [Blog Post]. Retrieved from https://thehealthcareblog.com/blog/2019/08/19/protecting-health-data-outside-of-hipaa-will-the-protecting-personal-health-data-act-tame-the-wild-west/

Rhodes, J. (2009). Using actor-network theory to trace an ICT (telecenter) implementation trajectory in an African women's micro-enterprise development organization. *Information Technologies & International Development, 5*(3), 1-20. Retrieved from https://itidjournal.org/index.php/itid.

Richardson, T. (2019, June 14). Senate privacy bill would expand HIPAA, restrict health apps. *Bloomberg Law*. Retrieved from https://news.bloomberglaw.com/privacy-and-data-security/lawmakers-float-federal-wearable-devices-privacy-legislation

Rodrigo, C. (2019, November 13). Google sparks new privacy fears over health care data. *The Hill.* Retrieved from https://thehill.com/policy/technology/470176-google-sparks-new-privacy-fears-over-health-care-data

U.S. Department of Health and Human Services. (2016, July). *Examining oversight of the*

privacy & security of health data collected by entities not regulated by HIPAA. Retrieved from https://www.healthit.gov/sites/default/files/non-covered_entities_report_june_17_2016.pdf

Young, L. (2018, May 18). There are thousands of health and fitness apps, and not much evidence they work: study. *Global News.* Retrieved from https://globalnews.ca/news/4215969/do-fitness-apps-work/

Zitomer, J. (2019, November 21). The future of healthtech – and how these companies are leading the pack [Blog post]. Retrieved from https://www.builtinnyc.com/2019/11/21/NYC-healthtech-advancements

BIBLIOGRAPHY

America's Health Insurance Plans. (2020, January). *Personal privacy outweighs increased transparency* [Press Release]. Retrieved from https://mms.businesswire.com/media/20200123005697/en/769272/1/202001-AHIP-MAPolling-FINAL.pdf?download=1

Anderson, D. (2020). *Current Actor Network Theory of protecting health data from businesses.* [Figure 2]. *STS Research Paper: Protecting Health Data Where Current Legislations Fall Short* (Unpublished undergraduate thesis). School of Engineering and Applied Science, University of Virginia. Charlottesville, VA.

Anderson, D. (2020). *Updated Actor Network Theory of protecting health data from businesses.* [Figure 3]. *STS Research Paper: Protecting Health Data Where Current Legislations Fall Short* (Unpublished undergraduate thesis). School of Engineering and Applied Science, University of Virginia. Charlottesville, VA.

Anderson, D. (2020). *U.S. federal legislations that protect consumers.* [Figure 1]. *STS Research Paper: Protecting Health Data Where Current Legislations Fall Short* (Unpublished undergraduate thesis). School of Engineering and Applied Science, University of Virginia. Charlottesville, VA.

Anderson, D (2019). *CBM-I and Implementation Intentions.* [Figure 1]. *Prospectus* (Unpublished undergraduate thesis). School of Engineering and Applied Science, University of Virginia. Charlottesville, VA.

Austin, P. (2019, November 4). The real reason google is buying Fitbit. *Time.* Retrieved from https://time.com/5717726/google-fitbit/

Bandelow, B. & Michaelis, S. (2015). Epidemiology of anxiety disorders in the 21st century. *Dialogues in Clinical Neuroscience, 17*(3), 327-335. Retrieved from https://www.dialogues-cns.org/

Bindley, K. (2019, November 22). Your health data isn't as safe as you think. *The Wall Street Journal.* Retrieved from https://www.wsj.com/articles/your-health-data-isnt-as-safe-as-you-think-11574418606?shareToken=st7af4b9d50fa34e1c9f28bfb69e99b736&reflink=article_email_share

Butler, M. (2017). Is HIPAA outdated? While coverage gaps and growing breaches raise industry concern, others argue HIPAA is still effective. *Journal of AHIMA, 88*(4), 14-17, 52. Retrieved from https://bok.ahima.org/

Chabinsky, S. & Pittman, F. (2019, March 7). *USA: Data protection 2019.* Retrieved from https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa

The Facebook scandal could change politics as well as the Internet. (2018, March 22). *The Economist.* Retrieved from https://www.economist.com/united-states/2018/03/22/the-facebook-scandal-could-change-politics-as-well-as-the-internet

Fair, L. (2019, July 24). FTC's $5 billion Facebook settlement: Record-breaking and history-making [Blog Post]. Retrieved from https://www.ftc.gov/news-events/blogs/business-blog/2019/07/ftcs-5-billion-facebook-settlement-record-breaking-history

Finley, K. (2015, October 6). Thank (or blame) Snowden for Europe's big privacy ruling. *Wired.* Retrieved from https://www.wired.com/2015/10/tech-companies-can-blame-snowden-data-privacy-decision/

Federal Trade Commission. (2015, January). *Internet of things: Privacy & security in a connected world.* Retrieved from https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

Global Market Insights, Inc. (2019, March 6). Worldwide digital health market to hit $504.4 billion by 2025: Global Markets Insights, Inc. *PR Newswire*. Retrieved from https://www.prnewswire.com/news-releases/worldwide-digital-health-market-to-hit-504-4-billion-by-2025-global-market-insights-inc-300807027.html

Harrod, J. (2019, May 15). Health data privacy: Updating HIPAA to match today's technology challenges [Blog post]. Retrieved from http://sitn.hms.harvard.edu/flash/2019/health-data-privacy/

Harvey, A. G., & Gumport, N. B. (2015). Evidence-based psychological treatments for mental disorders: Modifiable barriers to access and possible solutions. Behaviour research and therapy, *68*, 1-12.

Kang, C. (2019, March 8). The man deciding Facebook's fate. *The New York Times.* Retrieved from https://www.nytimes.com/2019/03/08/technology/ftc-facebook-joseph-simons.html

Klobuchar, A. & Murkowski, L. (2019). *Protecting personal health data act*. Retrieved from https://src.bna.com/I7O

Linder, D. (2019). The right to privacy [Blog Post]. Retrieved from http://law2.umkc.edu/faculty/projects/ftrials/conlaw/rightofprivacy.html

MacLeod, C. (2012). Cognitive bias modification procedures in the management of mental health disorders. *Current Opinion Psychiatry, 25*(2), 114-120.

doi:10.1097/YCO.0b013e32834fda4a

Marshall, J., Dunstan, D., & Bartik, W. (2019). The digital psychiatrist: In search of evidence-based apps for anxiety and depression. *Frontiers in Psychology, 10,* 831. doi:10.3389/fpsyt.2019.00831

McGraw, D, & Kuraitis, V. (2019, August 19). Protecting health data outside of HIPAA: Will the Protecting Personal Health Data Act tame the Wild West? [Blog Post]. Retrieved from https://thehealthcareblog.com/blog/2019/08/19/protecting-health-data-outside-of-hipaa-will-the-protecting-personal-health-data-act-tame-the-wild-west/

Miloff, A., Marklund, A., Carlbring, P. (2015). The challenger app for social anxiety disorder: New advances in mobile psychological treatment. *Internet Interventions, 2,* 382-391. doi:10.1016/j.invent.2015.08.001

NAMI. (2019, September). Mental Health by the Numbers | NAMI: National Alliance on Mental Illness. Retrieved September 17, 2019, from https://www.nami.org/learn-more/mental-health-by-the-numbers

Parker, L., Halter, V., Karliychuk, T., & Grundy, Q. (2019). How private is your mental health app data? An empirical study of mental health app privacy policies and practices. *International Journal of Law and Psychiatry, 64,* 198-204. doi:10.1016/j.ijlp.2019.04.002

Price, M., Yuen, E.K., Goetter, E.M., Herber, J.D., Forman, E.M., Acierno, R., & Ruggiero, K.J. (2013). mHealth: A mechanism to deliver more accessible, more effective mental health care. *Clinical Psychology & Psychotherapy, 21*(5), 427-436. doi:10.1002/cpp.1855

Richardson, T. (2019, June 14). Senate privacy bill would expand HIPAA, restrict health apps. *Bloomberg Law.* Retrieved from https://news.bloomberglaw.com/privacy-and-data-security/lawmakers-float-federal-wearable-devices-privacy-legislation

Robillard, J.M., Feng, T.L., Sporn, A.B., Lai, J. Lo, C. Ta, M., & Nadler R. (2019). Availability, readability, and content of privacy policies and terms of agreements of mental health

apps. *Internet Interventions, 17,* doi:10.1016/j.invent.2019.100243

Rodrigo, C. (2019, November 13). Google sparks new privacy fears over health care data. *The Hill.* Retrieved from https://thehill.com/policy/technology/470176-google-sparks-new-privacy-fears-over-health-care-data

U.S. Department of Health and Human Services. (2016, July). *Examining oversight of the privacy & security of health data collected by entities not regulated by HIPAA*. Retrieved from https://www.healthit.gov/sites/default/files/non-covered_entities_report_june_17_2016.pdf

Voss, W.G. & Houser, K.A. (2019) Personal data and the GDPR: Providing a competitive advantage for U.S. companies. *American Business Law Journal, 56*(2), 287-344. doi:10.1111/ablj.12139

Young, L. (2018, May 18). There are thousands of health and fitness apps, and not much evidence they work: study. *Global News.* Retrieved from https://globalnews.ca/news/4215969/do-fitness-apps-work/

Zitomer, J. (2019, November 21). The future of healthtech – and how these companies are leading the pack [Blog post]. Retrieved from https://www.builtinnyc.com/2019/11/21/NYC-healthtech-advancements