HELP US, HELP YOU:
BIG TECH AND THE FUTURE OF PERSONAL HEALTH RECORDS

CLAY BREWER

I. INTRODUCTION

Ed Dentel went to his local primary care physician due to chest pains.[1] The physician ran a few tests, but the results were all normal.[2] Perhaps he should change his diet? Get some exercise? But over the next few months, the chest pains continued.[3] Aware of the new health features in his new Apple Watch Series 4, such as the ECG app (electrocardiogram application), Ed decided to try it out.[4] The ECG is used to detect atrial fibrillation or A-fib for

[1] Michael Potuck, *New Development in case of Apple Watch customer who discovered heart condition with ECG app, featured on Good Morning America*, 9TO5MAC (Dec. 11, 2018), https://9to5mac.com/2018/12/11/apple-watch-ecg-saves-life-a-fib/.
[2] *Id.*
[3] *Id.*
[4] *Id.*

short.[5] In other words, the test analyzes the heart and detects whether there are any irregular heartbeats.[6] To his surprise, the watch detected A-fib, so Ed tried again.[7] The next morning, he tried again, and again, and again. Still A-fib. Switched wrists, no change. Then thinking that with a new device and knowing that Apple has said false positives are possible with all technology, Ed asked his wife to try it out.[8] No A-fib, no discrepancies with her readings.[9] Ed immediately drove to his local clinic, but, due to the wait, Ed almost decided to leave.[10] He cannot skip important meetings for work because of a dumb watch, can he? But he decided to wait it out. Ed explains that "he felt like a hypochondriac explaining that his watch told him something was wrong. But he was quickly given an ECG[11] by a technician, who called for a doctor." The watch was correct, the doctor read the results and responded, "Yup, you're in AFib.[12] This thing may have just saved your life."[13] Ed still believes if it were not for the

---

[5] *Id.*
[6] *See Medicine Plus: Atrial Fibrillation*, United States National Library of Medicine, https://medlineplus.gov/atrialfibrillation.html.
[7] Potuck, *supra* note 1.
[8] *Id.*
[9] *Id.*
[10] *Id.*
[11] The same technology used by the Apple Watch Series 4 is also used by physicians within the doctor's office. EKG and ECG are synonymous. The difference in acronym is based on whether the test name is translated from German elektro-kardiographie or from English electrocardiogram (ECG). *ECG vs. EKG: What's the Difference?*, NEUROSKY, (May 25, 2015), http://neurosky.com/2015/05/ecg-vs-ekg-whats-the-difference/.
[12] Potuck, *supra* note 1.
[13] *Id.*

Apple Watch, he could be dead having never returned to the physician.[14]

The intersection of technology and healthcare can bring individuals like Ed amazing benefits. But what about the risks of so much personal medical data being available to these same companies that claim to advance our well-being? Tim Cook, the CEO of Apple, believes that privacy is a fundamental human right and that Apple seeks to enrich the lives of individuals and provide great products, not make the individual the product. Mr. Cook stated in a recent interview with CNBC's Jim Cramer, "[w]e are taking what has been with the institution and empowering the individual to manage their health."[15] But what if Mr. Cook and Apple did not have these views? What if they suddenly believed that the customer was, in fact, now the product? Could they change this policy without any legal repercussions? The answer, in short, is yes.

For example, the sudden rise in 23andme, a company that tests your DNA to trace your genetics,[16] can perhaps be more illustrative of the risks presented to an individual's privacy. The

---

[14] *Id*.
[15] Lauren Fiener, *Apple CEO Tim Cook speaks with CNBC's Jim Cramer: Full transcript*, CNBC, (Updated Jan. 9, 2019), https://www.cnbc.com/2019/01/08/apple-ceo-tim-cook-interview-cnbc-jim-cramer-transcript.html.
[16] 23andme Media Center, (2019), https://mediacenter.23andme.com.

delivery man drops a small package off at your home.[17] A vial kit is contained inside.[18] You open the box, take out the vial, and spit into the vial.[19] You then follow the instructions and register the vial's barcode on 23andme's website, the kit is placed back in the mail with a sample of your saliva in the vial, and sent back to the laboratory for testing.[20] Your results will be returned in three to five weeks.[21] And "[i]n each drop of spit lies a whole story of ancestry, health, and connectedness that is about to unfold."[22] This all appears to be quite harmless and reveals many curiosities about ourselves and our family history. But in the words of iconic college football Coach Lee Corso[23], "not so fast, my friend."[24]

Once the results are received, where did the saliva sample go? Where are the DNA records filed? Unbeknownst to many, 23andme and others can sell your anonymized information they retrieve to third parties, and pharmaceutical company

---

[17] 23andme: How it Works, (2019), https://www.23andme.com/howitworks/.
[18] *Id.*
[19] *Id.*
[20] *Id.*
[21] *Id.*
[22] 23andme, *supra* note 16.
[23] Legendary college football coach and co-host of ESPN's College GameDay television show. https://espnmediazone.com/us/bios/corso_lee/.
[24] Ava Wallace, *Not so fast, my friend: A Stroke couldn't rob ESPN's Lee Corso of 'College Gameday'*
WASHINGTON POST (Oct. 14, 2017),
https://www.washingtonpost.com/news/sports/wp/2017/10/14/not-so-fast-my-friend-a-stroke-couldnt-rob-espns-lee-corso-of-college-gameday/?utm_term=.5e0baae9a7a6.

GlaxoSmithKline[25] has a $300 million stake in 23andme.[26] Does it make sense that the ordinary individual is required to explicitly opt-out in order to prevent their data from being shared with such pharmaceutical companies? When was the last time any of us actually read the terms and conditions of a product anyways? Or, if we did, if we actually understood it? So much for "informed consent."

The use of such technology undoubtedly brings remarkable results.[27] But there is more to it than the ordinary individual may know. What if large corporations could discover this medical information or, better yet, we freely gave it to them? What if such companies could then sell this information to large databases or simply the highest bidder? Initially, most would shrug this off. I have nothing to hide. So what if someone knows I went to the doctor last week for a cold or to have a plantar wart removed? But

---

[25] "[GlaxoSmithKline] ha[s] 3 global businesses that research, develop, and manufacture innovative pharmaceutical medicines, vaccines and consumer healthcare products." GlaxoSmithKline, (2019), https://www.gsk.com/en-gb/about-us/.

[26] Erin Brodwin, *DNA-testing company 23andMe has signed a $300 million deal with a drug giant. Here's how to delete your data if that freaks you out*, (July 25, 2018), https://www.businessinsider.com/dna-testing-delete-your-data-23andme-ancestry-2018-7; *GSK and 23andme sign agreement to leverage genetic insights for the development of novel medicines*, (July 25, 2018), https://www.gsk.com/en-gb/media/press-releases/gsk-and-23andme-sign-agreement-to-leverage-genetic-insights-for-the-development-of-novel-medicines/.

[27] *5 Ways Technology is Improving Health*, UNIVERSITY OF ILLINOIS AT CHICAGO: HEALTH INFORMATICS BLOG, (last visited January 27, 2019), https://healthinformatics.uic.edu/blog/5-ways-technology-is-improving-health/.

if this information is accessible, then what other information might be? Who has access? What inferences could arise?

The rise of cybercrime targeting healthcare further highlights the high demand for private health information.[28] For example, in July 2018, Singapore's Ministry of Health reported that hackers accessed and exported the personal health records of 1.5 million patients, including the health records of Prime Minister Lee Hsien Loong.[29] Through this breach, the hackers were able to extract specific "data on outpatient-dispensed medications" of 160,000 patients including the prime minister.[30] According to CNBC, medical records continue to be a hot commodity on the dark-web receiving sometimes three times or more as much per record as compared to Social Security numbers.[31] If these are the prices on the dark-web, imagine the heightened prices for legally

---

[28] Kate O'Flaherty, *Why Cyber-Criminals Are Attacking Healthcare - - And How to Stop Them*, FORBES, (Oct. 5, 2018), https://www.forbes.com/sites/kateoflahertyuk/2018/10/05/why-cyber-criminals-are-attacking-healthcare-and-how-to-stop-them/#d2da6c7f69eb.

[29] Jessica Davis, *Hackers breach 1.5 million Singapore patient records, including the prime minister's*, HEALTHCARE IT NEWS, (July 20, 2018), https://www.healthcareitnews.com/news/hackers-breach-15-million-singapore-patient-records-including-prime-ministers.

[30] *Id.*

[31] Jill Cornfield, *The dark web is a fraudster's bargain-hunting paradise*, CNBC, (July 2, 2018), https://www.cnbc.com/2018/06/29/the-dark-web-is-a-fraudsters-bargain-hunting-paradise.html; *See Medical Data: One Of The Hottest Commodities On The Dark Web*, SOURING EAGLES CONSULTING DATABASE BLOG, (May 30, 2018), https://soaringeagle.biz/medical-data-hot-commodity-on-dark-web/; Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN, (Updated April 9, 2018), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/

obtained medical information that we consent, often unwittingly, to give up.

However, the future appears to hold more technology involved within healthcare, not less.[32] And the explicit desires of tech powerhouses such as Apple, Amazon, and Alphabet's Google to address the problems of the American healthcare system appear to bring forth significant benefits.[33] The growth of technology over the last decade has developed a society more connected than ever before.[34] From monitoring your heart on an Apple Watch to receiving your prescriptions via Amazon Prime, and flagging potentially future medical issues with Google's artificial intelligence, the benefits seem infinite if they can become a

[32] Erica Bettencourt, *Technology Trends Are The Future For Healthcare*, DIVERSITYNURSINGBLOG, (March 15, 2018), http://blog.diversitynursing.com/blog/these-technology-trends-are-the-future-for-healthcare.
[33] Natasha Singer, *How Big Tech Is Going After Your Health Care*, NY TIMES, (Dec. 26, 2017), https://www.nytimes.com/2017/12/26/technology/big-tech-health-care.html.
[34] Sean Illing, *Technology isn't just changing society–it's changing what it means to be human: A conversation with historian of science Michael Bess*, VOX, (Feb. 23, 2018), https://www.vox.com/technology/2018/2/23/16992816/facebook-twitter-tech-artificial-intelligence-crispr; *The connected future: Internet of Things forecast*, ERICSSON MOBILITY REPORT, (last visited January 27, 2019), https://www.ericsson.com/en/mobility-report/internet-of-things-forecast.

reality.[35] Yet as the old proverb goes, "the road to hell is paved with good intentions."[36]

The more reliant society becomes on technology and the ever-growing Internet of Things ("IOT")[37], the more vulnerable society becomes to not only the traditional fears of cyberattacks ,but more so to the power that is freely granted to those corporations that possess such information with virtually no regulatory restraint.[38] Technology will only continue to grow within our daily lives.[39] And the convergence of technology and healthcare demonstrates the ever-expanding tentacles of big tech.[40]

This note will address the issues that will inevitably arise as this convergence of tech and healthcare continue. Part I will discuss a few of the current laws and regulations that seek to

---

[35] Dylan Scott, *Why Apple, Amazon, and Google are making big health care moves: Silicon Valley wants to disrupt your health care*, VOX, (March 6, 2018), https://www.healthleadersmedia.com/finance/why-apple-amazon-and-google-are-making-big-health-care-moves.

[36] Soren Kierkegaard, *Works of Love*, (Charles E. Moore ed., *Provocations: Spiritual Writings of Kierkegaard*, 14, Plough Publishing House 2007) (1847) available at: http://www-astro.physics.ox.ac.uk/~ddarg/pdf/Provocations.

[37] "The Internet of Things is a network of physical objects–vehicles, machines, home appliances, and more–that use sensors and [application programming interfaces] to connect and exchange data over the Internet." *What is the Internet of Things (IoT)?*, SAP SE, (Feb. 19, 2019), https://www.sap.com/trends/internet-of-things.html.

[38] Barry R. Furrow, et al., *Health Law: Cases, Materials And Problems*, 174 (8th ed. 2018).

[39] According to a 2018 Nielsen Total Audience Report, "American adults spend over 11 hours per day listening to, watching, reading or generally interacting with media." *Time Flies: U.S. Adults Now Spend Nearly Half A Day Interacting With Media*, NIELSEN, (July 31, 2018), https://www.nielsen.com/us/en/insights/news/2018/time-flies-us-adults-now-spend-nearly-half-a-day-interacting-with-media.print.html.

[40] Nancy Huynh, *How the "Big 4" Tech Companies Are Leading Healthcare Innovation*, (Aug. 27, 2018), https://healthcareweekly.com/how-the-big-4-tech-companies-are-leading-healthcare-innovation/.

protect personal health records in the United States' and Europe, specifically in comparing the United States Health Insurance Accountability and Portability Act ("HIPAA") and the Health Information Technology for Economic and Clinical Health Act ("HITECH") with the European Union's much broader response to data privacy concerns via the General Data Protection Regulation ("GDPR").

To follow, Part II will introduce three of the tech giants– Apple, Amazon, and Google–to give a glimpse into their individual visions to tackle healthcare's most vexing problems while presenting how these companies will test the current legal framework of medical data privacy. Lastly, Part III will provide initial thoughts to restructure the current legal framework for private health information in the United States similarly to that of the European Union in order to protect an individual while also seeking to not stifle big tech's health innovation, but to enable it.

Part I: The Law As We Know It

HIPAA & HITECH

In 1996, Congress passed and President Bill Clinton signed into law the Health Insurance Portability and Accountability Act ("HIPAA"), which would "ensure the portability of health benefits when workers change or lose their jobs and will protect workers against discrimination by health plans based on their health

status."[41] However, the turn of the millennium welcomed "the rise of electronic record keeping and the Internet" increasing the need to better streamline the transmission of health records, and for greater privacy and security of an individual's medical data.[42]

To meet the guidelines established in HIPAA, the Department of Health and Human Services ("HHS") promulgated the Privacy[43] and Security Rules.[44] In the initial preamble to the Privacy Rule in 2000, HHS identified three major purposes for the newly promulgated regulation:

> "(1) To protect and enhance the rights of consumers by providing them access to their health information and controlling inappropriate use of that information; (2) to improve the quality of health care in the U.S. by restoring trust in the health care system among consumers, health care professionals, and the multitude of organizations and individuals committed to the delivery of care; and (3) to improve the efficiency and effectiveness of health care delivery by creating a national framework for health privacy protection that builds on efforts by states, health systems, and individual organizations and individuals."[45]

---

[41] *Statement on Signing the Health Insurance Portability and Accountability Act of 1996*, University of California at Santa Barbara: The American Presidency Project, https://www.presidency.ucsb.edu/documents/statement-signing-the-health-insurance-portability-and-accountability-act-1996.
[42] Furrow, *supra* note 39, at 172.
[43] HIPAA Privacy Rule, 45 C.F.R. §§ 160, 164 (2013).
[44] HIPAA Security Rule, 45 C.F.R. § 164(c) (2013). The Security Rule will not be discussed further in this note, but "sets forth standards for keeping health data secure, including encryption and other technological and organizations requirements." Furrow, *supra* note 39, at 172.
[45] Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82462 (Dec. 28, 2000).

These rules were an effort to promote the industry as a whole to adopt electronic health record ("EHR") systems.[46] However, from reluctance to change to the costs associated with adopting EHR, the optimism that existed did not catch on as originally hoped.[47] This led to the enactment of the Health Information Technology for Economic and Clinical Health Act ("HITECH") in 2009, which sought to catalyze EHR adoption across the country as well as establish a structure for notifying the public and HHS about data breaches and the protection of an individual's private health information ("PHI"). [48] HITECH provided the Office of the National Coordinator for Health Information Technology ("ONC") the power to begin offering financial incentives in 2011 to providers that adopted EHR and demonstrated meaningful use of such technology,[49] but would impose penalties on those providers that had yet to adopt EHR by 2015.[50] The HITECH amendments of 2009 were implemented through the Omnibus HIPAA rulemaking of 2013[51] that led to the Privacy Rule's current form while also linking the Privacy Rule with the Security Rule, the Enforcement Rule,[52] and the Breach Notification Rule.[53]

---

[46] Furrow, *supra* note 39, at 172-73.
[47] *Id.* at 193.
[48] *Id.* at 190.
[49] 42 U.S.C. §§ 300jj to jj-51 (2016).
[50] 42 U.S.C. § 1320d-5 (2009).
[51] 45 C.F.R. Part 160, Subpart D (2013).
[52] 42 U.S.C. §§ 300jj to jj-51.
[53] 42 C.F.R. §§ 164.400 to 164.414 (2009).

The Privacy Rule will be the primary focus of this note's HIPAA discussion. In order to adequately understand how the big technology companies can impact the current legal framework, one must first understand what is currently covered under the Privacy Rule.

The most significant definitions of the Privacy Rule include: (1) protected health information; (2) covered entities; and (3) business associates.[54] Protected health information, also known as individually identifiable health information, has an expansive definition but can be understood to include an individual's health information "created or received by a health care provider, health plan, employer, or health care clearinghouse" that identifies or reasonably could be used to identify a particular individual.[55] In contrast to the broad definition of protected health information, the entities that are subject to HIPAA are significantly limited in regards to the ever-growing landscape of technology companies that have continued to enter the health sphere since the Privacy Rule's beginning in 2002 and its latest iteration in 2013.[56] Covered entities are defined under HIPAA as a health plan;[57] a health care

[54] Farrow, *supra* note 39.
[55] *Id.* at § 160.103-Definitions.
[56] *Guidance on HIPAA & Cloud Computing*, Dept. of Health and Human Servs., https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html.
[57] Examples include: health insurance companies, health management organizations. (HMOs), company health plans, and government programs that

clearinghouse;[58] or a health care provider that transmits any health information in electronic form in connection with a transaction.[59] Business associates are entities that "on behalf of a covered entity . . . creates, receives, maintains, or transmits protected health information for a function or activity regulated by [HIPAA]."[60] The "on behalf of" language is a key part of the business associate definition analysis because if the entity is operating exclusively with consumers, (i.e., Apple, Amazon, or Google) then HIPAA would not apply unless the current definition of covered entity were to change.[61]

HIPAA and its related rules and regulations "set[ ] a floor of ground rules for health care providers, health plans, and health care clearinghouses to follow, in order to protect patients and encourage them to seek needed care."[62] In other words, this means that entities that fall under HIPAA are obligated to comply but also may fall subject to more stringent state laws.[63] As a result of this

---

pay for health care, such as Medicare and Medicaid. https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html.

[58] Examples include: "entities that process nonstandard health information they receive from another entity into a standard (i.e., standard electronic format or data content), or vice versa. https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html.

[59] Examples include: doctors, clinics, psychologists, and dentists "but only if they transmit any information in an electronic form in connection with a transaction for which HHS has adopted a standard." https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html.

[60] HIPAA Privacy Rule, 45 C.F.R. §§ 160, 164.

[61] Dept. of Health & Human Servs., s*upra* note 56.

[62] Furrow, *supra* note 39, at 174.

[63] Stephanie Baum, *Lawyer: It's time to pre-empt state medical privacy laws that differ from HIPAA*, MEDCITY NEWS ,(April 29, 2017),

potentiality, there could be fifty additional laws for entities to comply with while also complying with HIPAA. At the time the preamble to the Privacy Rule was written, "[r]ules requiring the protection of health privacy in the United States ha[d] been enacted primarily by the states . . . . [but the Privacy Rule] establish[ed] for the first time a set of basic national privacy standards . . . that provide[d] all Americans with a basic level of protection."[64] However revolutionary the Privacy Rule may have been at the time of the preamble's presentation, technology has changed significantly causing this national standard an annoyance as opposed to a protective data privacy regulation because the big tech companies now entering the arena are not necessarily being covered. Additionally, the possibility of a multitude of state laws causes difficulty for companies to continue to innovate and abide by separate regulations depending on the location or citizenry of the business operation.[65] As a result, many tech CEOs expressed their support for a national standard before Congress with the condition that state laws such as that of California[66] would be

---

https://medcitynews.com/2017/04/lawyer-time-pre-empt-state-medical-data-privacy-laws-differ-hipaa/?rf=1

[64] 65 Fed. Reg. 82642.

[65] David Shepardson, *Tech companies back U.S. privacy law if it preempts California's*, REUTERS, (Sept. 26, 2018), https://www.reuters.com/article/us-usa-tech-congress/tech-companies-back-u-s-privacy-law-if-it-preempts-californias-idUSKCN1M62TE.

[66] *Id.* "California Governor Jerry Brown signed [a] data privacy [law] aimed at giving consumers more control over how companies collect and manage their personal information."

preempted. [67] The California law, known as the California Consumer Privacy Act of 2018, will go into effect in 2020 and for purposes of this note can be similarly linked to that of the GDPR in Europe.[68]

Lastly, even assuming HIPAA covers much of the information and entities that would raise concerns for the individual in regards to their personal medical data, "there is no private right of action for individuals whose information has been used or disclosed in violation of the law."[69] The Office of Civil rights under HHS is given the regulatory authority to investigate such violation and state attorneys general are also permitted to do so by filing in federal district court due to HIPAA being a federal law. [70] Preventing a private right of action may prevent the common cliche of "flooding the courts" but does little to empower the individual in owning their personal information. The enforcement powers being placed solely in the hands of elected officials or regulatory career officers places the rights of the individual to the subjective decisions of others. Moreover, a part of the 2013 Omnibus HIPAA Rule, there are possible criminal penalties for "[a] person who knowingly obtains or discloses

---

[67] *Id.*
[68] Kristen J. Matthews and Courtney M. Bowman, *The California Consumer Privacy Act of 2018*, PRIVACY LAW BLOG, (July 13, 2018), https://privacylaw.proskauer.com/2018/07/articles/data-privacy-laws/the-california-consumer-privacy-act-of-2018/.
[69] Furrow, *supra* note 39, at 189.
[70] 42 U.S.C. § 1320d-5 (2013).

individually identifiable health information in violation of HIPAA,"[71] and civil penalties that an "annual maximum of $1.5 million for a violation."[72] For a large corporation making billions every quarter, this is hardly a disincentive.

GDPR

Events like Yahoo's data breach that exposed private information of millions of Yahoo email users[73], and the disclosure that Facebook user data was directly shared with third parties like Cambridge Analytica[74], revealed how exposed technology can make an individual, bringing the world of 1984[75] from fiction to reality.

The European Union put into effect the General Data Protection Regulation ("GDPR")[76] on May 25, 2018.[77] The twenty-eight member countries[78] of the European Union implemented this

---

[71] 45 C.F.R. § 160.408 (2013).
[72] 45 C.F.R. § 160.404 (2016).
[73] Oath: A Verizon Company, *Yahoo provides notice to additional users affected by previously disclosed 2013 data theft*, (Oct. 3, 2017), https://www.oath.com/press/yahoo-provides-notice-to-additional-users-affected-by-previously/.
[74] Andrea Valdez, *Everything You Need to Know About Facebook and Cambridge Analytica*, WIRED (March 23, 2018), https://www.wired.com/story/wired-facebook-cambridge-analytica-coverage/; Vindu Goel, *The Week in Tech: A Breach That Ripples Far Beyond Facebook*, NY TIMES (Oct. 5, 2018), https://www.nytimes.com/2018/10/05/technology/facebook-breach.html.
[75] George Orwell, 1984, (1949).
[76]Council Regulation 2016/679, of April 27, 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, 2016 O.J. (L 269).
[77] *EU GDPR,* https://eugdpr.org (last visited June 26, 2019).
[78] Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia,

revamped regulation to protect the personal data of citizens of the European Union ("EU"), to prevent invasions of privacy, and to empower the individual in owning their own data.[79] To put the GDPR in comparison to HIPAA, Reg Harnish, the CEO of GreyCastle Security,[80] writes that GDPR can go much further than HIPAA in both punitive fines and its scope of coverage because "[u]nlike HIPPA, which has a maximum fine penalty of $1.5 million per year[81] for violations of an identical provision, GDPR fines can cost up to $24 million or four percent of the violator's annual global revenue, whichever is greater."[82] In essence, these large punishments are focused on Europe's desire to "alter[ ] how businesses and public sector organizations [ ] handle the information of their customers. [while] also boost[ing] the rights of

---

Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden. European Union, https://europa.eu/european-union/about-eu/countries_en (last visited June 26, 2019). The United Kingdom is the twenty-eighth member of the EU but is in the process of leaving after the decision to leave prevailed in the June 23, 2016, referendum. (Author's note).

[79] The GDPR builds upon and replaces the 1995 data protection directive in order to modernize legislation with societal and technological advancements. In the words of the United Kingdom's information commissioner, Elizabeth Denham, "The GDPR is a step change for data protection . . . It's still an evolution, not a revolution."
Matt Burgess, *What is GDPR? The summary guide to GDPR compliance in the UK*, WIRED (January 21, 2019), https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018.

[80] Cybersecurity service company. *See* GreyCastle Security, https://www.greycastlesecurity.com/company/ (last visited June 26, 2019).

[81] 45 C.F.R. § 160.404.

[82] Reg Harnish, *7 Things Healthcare Organizations Need to Know About GDPR*, HIT CONSULTANT (March 21, 2018), https://hitconsultant.net/2018/03/21/healthcare-organizations-gdpr/; Commission Regulation (EU) 2016/679, Article 83, available at: https://gdpr-info.eu/art-83-gdpr/.

individuals and giv[ing the individual] more control over their information."[83] Stated more simply, the GDPR "is designed to (1) harmonize data privacy laws across Europe; (2) protect and empower all EU citizens data privacy; and (3) reshape the way organizations across the region approach data privacy."[84] For example, French authorities under the auspices of the GDPR implemented a $57 million fine against Google on January 21, 2019, the largest fine under the new law.[85] The European Union is currently made of twenty-eight members, which all individually may enforce the GDPR.[86] Under GDPR, "a big part of the new rule is a requirement that companies explain to users how their data is being collected and used, and in many cases seek consent from users to collect it."[87] As a result of this new regulatory power, France's National Data Protection Commission revealed that "Google violated rules requiring information about data collection to be transparent, and users to be sufficiently informed . . . in some cases requiring up to five or six clicks" for information to become discoverable" making the individual unlikely to pursue further and

---

[83] *See supra* note 79.
[84] *See* https://eugdpr.org. The actual link to the European Commission can be found at: https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en.
[85] Sam Schechner, *Google Fined $57 Million in Biggest Penalty Yet Under New European Law*, THE WALL STREET JOURNAL (Jan. 21, 2019), https://www.wsj.com/articles/google-fined-57-million-by-french-regulator-11548085558?mod=djemalertNEWS.
[86] Article 77, available at: https://gdpr-info.eu/art-77-gdpr/.
[87] *See supra* note 85.

resulting in Google not "obtain[ing] appropriate consent for personalized ads on Google's platforms."[88] From this example of Google, the central idea of the GDPR can be further understood to recognize that "not only will organisations [sic] have to ensure that personal data is gathered legally and under strict conditions, but those who collect and manage it will be obliged to protect it from misuse and exploitation, as well as respect the rights of data owners."[89]

Now with this central idea in mind, three key terms must be defined: (1) controllers; (2) processors; and (3) personal data. These can be loosely compared to HIPAA's current covered entity and business associate methodology.[90] Under Article 4 of the GDPR, controllers are defined as a "person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of processing of personal data;" while processors are defined as a "person, public authority, agency, or other body which processes personal data on behalf of the controller" with controllers also being held responsible to ensure that contracts with processors are GDPR compliant.[91]

---

[88] *See supra* note 85.
[89] Danny Palmer, *What is GDPR? Everything you need to know about the new general data protection regulations*, ZDNET (May 23, 2018), https://www.zdnet.com/article/gdpr-an-executive-guide-to-what-you-need-to-know/.
[90] Article 4, available at: https://gdpr-info.eu/art-4-gdpr/.
[91] *See supra* note 89.

Personal data as "any information that relates to an identified or identifiable living individual."[92]

Arguably the more important aspect of GDPR that distinguishes it from HIPAA and other like-situated American counterparts is determining what is covered and who must comply. Even though GDPR is a law implemented by the European Union, "the legislation extends further than the borders of Europe itself, as international organisations [sic] based outside the region but with activity on 'European soil' will still need to comply." [93] Interestingly enough, "[t]he European Commission claims that by having a single supervisor authority for the entire EU, it will make it simpler and cheaper for businesses to operate within the region."[94] The GDPR is similar to HIPAA in that it does not directly provide a private right of action for the individual, but it does establish two significant provisions that place great power within the individual's hands. The first is under Article 17 designated the right to erasure or, more colloquially, the 'right to be forgotten.'[95] Upon request by the individual, the company must erase the data they possess on the individual if one of six

---

[92] Examples include: a name and surname, a home address, an IP address, data held by a hospital or doctor, which could be a symbol that uniquely identifies a person. *See* https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en.
[93] *See supra* note 85.
[94] *Id*.
[95] Article 17, available at: https://gdpr-info.eu/issues/right-to-be-forgotten/.

conditions are met.[96] However, this idea does present challenges for medical data when all information can be considered impactful for further treatment. Secondly, Article 20 is designated the 'right of portability' granting the individual the right to gain access to the data companies have on them[97] with Article 21 providing the 'right to object' requiring companies to make it clear and precise for an individual to be able to opt-in or opt-out of sharing certain information[98]

Part II: The Big Three

The connection between of technology and healthcare has been a common topic since President Clinton signed HIPAA into law in 1996 with such a connection being premised upon the goals that healthcare policy revolves around: (1) cost, (2) quality, (3) access, and (4) choice.[99] However, technology has changed rapidly since 1996 and even since the 2013 HIPAA Omnibus.[100]

The difficulty in balancing these four goals has led to optimism with the entrance of large technology corporations–such as Apple, Amazon, and Google–bringing their connected user-base, extended consumer-data information, and hundreds of

---

[96] *Id*.
[97] Article 20, available at https://gdpr-info.eu/art-20-gdpr/.
[98] Article 21, available at https://gdpr-info.eu/art-21-gdpr/.
[99] *See supra* note 39, at 1.
[100] At the time of HIPAA in 1996, such items as the iPhone (2007), Fitbit (2007), iPad (2010), Samsung Galaxy S (2010), Apple Watch (2015) were likely linked closer to an episode of The Jetsons than reality. (Author's note).

billions of dollars to join the juggling act.[101] Apple, Amazon, and Google, three of the world's largest companies by market capitalization and name recognition,[102] come into contact with millions of individuals on a daily basis. From using the iPhone or Apple Watch and its various applications, to the commonly used Google search engine, from Amazon Prime[103] or walking into a Whole Foods[104], to Amazon's Web Services[105], individuals from all walks of life interact with these tech giants for nearly everything everyday. These companies are attempting to bring their successes within these various fields to the healthcare sector in order to remedy the difficult balancing act that is the American healthcare system.[106] However, success in one field does not guarantee success in another. Dan D'Orazio, CEO of healthcare

---

[101] Art Kleiner, *A Doctor's Prescription: Data May Finally Be Good for Your Health*, STRATEGY+BUSINESS (Oct. 8, 2018), https://www.strategy-business.com/article/A-Doctors-Prescription-Data-May-Finally-Be-Good-for-Your-Health?gko=e3c4e.

[102] Gil Press, *How Apple, Amazon, Facebook, Google And Microsoft Made 2018 The Year That IT Mattered A Lot*, FORBES (Dec. 30, 2018), https://www.forbes.com/sites/gilpress/2018/12/30/how-apple-amazon-facebook-google-and-microsoft-made-2018-the-year-that-it-mattered-a-lot/#3592eedb1cee.

[103] Amazon Prime is a paid for service subscription model that allows customers to receive free shipping from Amazon along with a variety of other benefits. *See generally* https://www.amazon.com/amazonprime?_encoding=UTF8&%2AVersion%2A=1&%2Aentries%2A=0.

[104] Amazon began its purchase of the national supermarket chain in 2017. Nick Wingfield and Michael J. de la Merced, *Amazon to Buy Whole Foods for $. 13.4 Billion*, NY TIMES (June 16, 2017), https://www.nytimes.com/2017/06/16/business/dealbook/amazon-whole-foods.html.

[105] Amazon Web Services (AWS) is Amazon's cloud computing platform that assists in analyzing large amounts of data, data storage, among other tasks. *See* generally https://aws.amazon.com.

[106] See s*upra* note 39.

research firm Sage Growth Partners[107], reiterates the belief of many currently within the healthcare industry: "We try to tell people that come in from outside that things don't necessarily translate well from other industries."[108] Professor Scott Galloway of New York University Stern School of Business takes a much more hostile approach designating three of these companies as a part of the four horsemen[109] and questioning their ability to free reign across society:

> "[w]e know these companies aren't benevolent beings, yet we invite them into the most intimate areas of our lives. We willingly divulge personal updates, knowing they'll be used for profit. Our media elevate the executives . . . Our governments grant them special treatment . . . So, are these entities the Four Horsemen of god, love, sex, and consumption?[110] Or are they the Four Horsemen of the apocalypse? The answer is yes to both questions."[111]

Because of the benefits technology has brought to our lives and can bring to healthcare, this note does not go as far as Professor Galloway to all but indict big tech power. But this note

---

[107] Marketing and growth consulting firm for healthcare organizations. *See* http://sage-growth.com/index.php/about/.
[108] Klint Finley, *Embattled Tech Companies Charge Deeper Into Health Care*, WIRED (March 1, 2018), https://www.wired.com/story/embattled-tech-companies-charge-deeper-into-health-care/.
[109] Scott Galloway, The Four: The Hidden DNA Amazon, Apple, Facebook, and Google, (1st ed. 2017). Professor Galloway's fourth horseman is Facebook, but Facebook will not be addressed within this note. (Author's note).
[110] *Id.* at 3-5. In his book, Galloway argues that Google's Search capabilities make it like a god of information, Apple's luxury status appeals to sex, Facebook's social media presence of sharing appeals to our desire for love, and Amazon's vast array of options appeal to our desire to consume. (Author's note).
[111] *Id.* at 2.

does urge for restructuring the current regulatory framework for heath; fully understanding that not every CEO will have similar privacy beliefs as Apple's Tim Cook[112]. Many issues can arise with different companies entering healthcare such as increases in the difficulty of not only the interoperability[113] of the information across different platforms[114], but also the potentiality of these companies profiting off a patient's medical data.[115]

APPLE

In addressing privacy at the International Conference of Data Protection and Privacy Commissioners in Brussels, Belgium, Apple CEO Tim Cook urged for the adoption of stronger data

---

[112] Tim Cook has expressed multiple times that he believes, and that Apple as a company believes, that privacy is a fundamental human right. Jim Vincent, *Tim Cook warns of 'data-industrial complex' in call for comprehensive US privacy laws*, THE VERGE (Oct. 24, 2018), https://www.theverge.com/2018/10/24/18017842/tim-cook-data-privacy-laws-us-speech-brussels.

[113] The extent to which devices and networks can talk to one another. One way of thinking about this would be to think of the difficulties one may commonly have converting documents created on Apple's Pages interface versus Microsoft's Word. Competing companies make different software and have different operations. Many do not freely create universally compatible products to specifically not promote the use of a competitor. *See generally* https://www.himss.org/library/interoperability-standards/what-is-interoperability.

[114] Although beyond the scope of this note, it is important to know that information blocking can be a serious issue with rivals not permitting incompatible software to relate use its databases preventing health care providers from accessing all of an individual's records. Congress has attempted to remedy the situation in the 21st Century Cures Act with the Office of Management and Budget reviewing a proposed rule from the Office of the National Coordinator. *See generally* Mandy Roth, *Countdown To Information Blocking Rule In Progress*, HEALTH LEADERS MEDIA (Sept. 28, 2018), https://www.healthleadersmedia.com/innovation/countdown-information-blocking-rule-progress.

[115] *See supra* note 26.

protection within the United States.[116] First, Cook discussed the wonders of good that technology has brought to individuals but followed with a warning for the future:

> "[W]e see vividly–painfully–how technology can harm rather than help. Platforms and algorithms that promised to improve our lives can actually magnify our worst human tendencies. Rogue actors and even governments have taken advantage of user trust to deepen division, incite violence, and even undermine our shared sense of what is true and what is false.
>
> . . . .
>
> And those of us who believe in technology's potential for good must not shrink from this moment. Now more than ever . . . we must ask ourselves a fundamental question: What kind of world do we want to live in?"[117]

This small excerpt alone can cause one to pause and truly think about the type of control that technology has over an individual's daily life. As of February 1, 2018, Apple announced that there are 1.3 billion actively used Apple products in the world.[118] According to the United States Census Bureau, there are roughly 7.53 billion people in the world.[119] As a result, Apple has roughly 17% as many devices in use as there are individuals in the world.

---

[116] Apple Holic, *Complete Transcript, video of Apple CEO Tim Cook's EU privacy speech*, COMPUTERWORLD https://www.computerworld.com/article/3315623/security/complete-transcript-video-of-apple-ceo-tim-cooks-eu-privacy-speech.html.
[117] *See supra* note 103.
[118] Juli Clover, *Apple Now Has 1.3 Billion Active Devices Worldwide*, MACRUMORS (Feb. 1, 2018), https://www.macrumors.com/2018/02/01/apple-now-has-1-3-billion-active-devices-worldwide/. Apple press release available at: https://www.apple.com/newsroom/2018/02/apple-reports-first-quarter-results/.
[119] United States Census Bureau, https://www.census.gov/popclock/, (last visited January 27, 2019).

In previous years and continuing into 2019, Apple has hired dozens of doctors to assist in the company's entrance into healthcare.[120] With the growing features from the Health App on the iPhone to the health focus abilities of the Apple Watch Series 4, Apple is demonstrating its commitment to growing its focus from purely wellness and fitness to essentially a health company.[121] There is no question that Mr. Cook is pushing Apple in a direction that he proclaims will have individuals look back on these times and truly believe that Apple's greatest contribution to mankind was health.[122] So where does this contribution begin?

First, Apple has continued to gain more and more recognition for its innovative fifth iteration of the Apple Watch with the introduction of the Apple Watch Series 4 in the fall of 2018.[123] Apple displays the new Apple Watch as "inspir[ing] you to live a healthier life by helping you manage everything from everyday stress to calories burned" while also introducing the new

---

[120] Christina Farr, *Apple now has dozens of doctors on staff, showing it's serious about health tech*, CNBC (Dec. 12, 2018), https://www.cnbc.com/2018/12/12/apple-has-dozens-of-doctors-on-staff.html.
[121] *Id.*
[122] Chance Miller, *Tim Cook teases 'new services' coming in 2019, says Apple's 'greatest contribution to mankind' will be health-related*, 9TO5MAC (Jan. 8, 2019), https://9to5mac.com/2019/01/08/tim-cook-services-health-care/.
[123] Kathleen Felton, *The Apple Watch Series 4: Everything You Need to Know About the Game-Changing New Health Features*, HEALTH (Sept. 13, 2018), https://www.health.com/condition/heart-disease/apple-watch-series-4; Chance Miller, *Apple officially announces Apple Watch Series 4 with larger display, thinner body, more*, 9TO5MAC (Sept. 12, 2018), https://9to5mac.com/2018/09/12/apple-watch-series-4-announced-release-price/; Sara Salinas, *Apple adds heart monitoring to Apple Watch*, CNBC (Sept, 12, 2018), https://www.cnbc.com/2018/09/12/apple-watch-series-4.html.

ECG[124] app that "is capable of generating an ECG similar to a single-lead electrocardiogram."[125] Apple is focused on enriching the lives of individuals across the world by enabling individuals to take a proactive approach towards their health. Within 30 seconds, the ECG app can indicate whether your heart rhythm shows signs of atrial fibrillation–a serious form of irregular heart rhythm" while keeping all such data from the Apple Watch encrypted on the device for the individual's personal use and ability to share with whom the individual so chooses.[126] In other words, Apple freely chooses to keep an individual's personal data on the device, there is no law or regulation making this mandatory.

Apple also recently introduced the fall detection feature on the Apple Watch that uses the accelerometer and gyroscope to create "a hard fall alert" to "easily initiate a call to emergency services[,] dismiss the alert[,or i]f you're unresponsive after 60 seconds, the emergency call will be placed automatically and a message with your location will be sent to your emergency contacts."[127] There is no doubt that such capabilities have already produced significant results with the ECG feature–described in the

---

[124] *See supra* note 11.
[125] *See generally* https://www.apple.com/apple-watch-series-4/health/.
[126] *Id.*
[127] *Id.*

introduction of this note–causing an individual to go to the doctor and discover his atrial fibrillation and potentially saving his life.[128]

Second, Apple highlights its Health App that links Activity[129], Sleep[130], Mindfulness[131], and Nutrition[132] as an easily accessible platform stored on an individual's iPhone that "consolidate[ ] health data from iPhone, Apple Watch, and third-party apps you already use . . . . And it recommends other helpful apps . . . making it simpler than ever to move your health forward."[133] The Health App "makes it easy to keep tabs on a wide array of data . . . from measurements of your blood pressure and blood glucose to records for your weight and reproductive health."[134] These capabilities will also permit the patient to keep one's health records–such as lab results and immunizations–within one place from multiple institutions.[135] As with the majority of Apple's services, an individual's personal information such as Touch ID[136], FaceID[137], and personal health information is stored

---

[128] *See* s*upra* note 1.
[129] *See* https://www.apple.com/ios/health/.
[130] *Id.*
[131] *Id.*
[132] *Id.*
[133] *Id.*
[134] *Id.*
[135] Participating health institutions can be found at https://support.apple.com/en-us/HT208647. Essentially empowering the individual to own their data and present it to the doctor as opposed to it being stored elsewhere. (Author's note).
[136] TouchID is the ability of the individual to use their fingerprint to unlock their Apple devices and approve certain actions such as payments. *See* https://support.apple.com/en-us/HT201371.

on the individual's device and encrypted on the device itself and while in transit between devices.[138] This commitment to encryption and customer privacy is created to prohibit even Apple from accessing such data without the individual's explicit permission.[139] But remember, this is an Apple policy decision and not mandated by any law or regulation. However, Apple warns the user that "[a]pps that access HealthKit are required to have a privacy policy, so be sure to review these policies before providing apps with access to your health and fitness data."[140] An inference that one may use to identify that Apple is aware that HIPAA does not apply to these types of records unless a HIPAA covered party is present.

Moreover, Apple permits individuals to explicitly opt-into "a software framework for apps [designated ResearchKit] that let medical researchers gather robust and meaningful data" from the individual to better improve diagnoses and cures going forward and CareKit that is "a software framework for apps that let you better understand and manage your medical conditions" further enabling individuals to take advantage of their freedom to choose.[141] Such research capabilities through this platform has permitted app creators to further understand the effects and

---

[137] FaceID is a continuation of the TouchID technology idea that uses sensor technology to do the same things. As TouchID but with an individual's face when looking at the device. See https://support.apple.com/en-us/HT208108.
[138] *See* https://www.apple.com/privacy/approach-to-privacy/.
[139] *See* s*upra* note 116.
[140] *Id.*
[141] *See* https://www.apple.com/researchkit/.

possible remedies to Parkinson's disease using the iPhone's "gyroscope and other iPhone features to measure dexterity, balance, gait, and memory" and also using "front-facing HD camera in iPhone, along with innovative facial recognition algorithms" to assist in diagnosing and treating autism earlier without the need for always going to a specialist.[142]

The notion presented by Tim Cook that society will look back on Apple and believe that their greatest contribution was health, from these few examples above, appears to be not too far from reality. The self-regulation that Apple's policy implements to protect a user's privacy is more of an exception to the rule as opposed to the rule itself. The two remaining companies will flirt more with the line due to their business models in health focusing more on data collection and artificial intelligence as opposed to providing software with their own personal hardware products. But in continuing, it is crucial to remember that a policy is not a mandated law.[143]

AMAZON

Amazon has a much different approach than Apple and is focused on what it can do in the future in regards to utilizing

---

[142] *Id.*

[143] Carolyn Beeler, *Who gets access to the data my Apple Watch collects?*, WHYY (April 30, 2015), https://whyy.org/segments/who-gets-access-to-the-data-my-apple-watch-collects/.

software and the expansion of its cloud[144] platform, Amazon Web Services ("AWS"), while also seeking to grow its e-commerce scope to provide individuals with more affordable drugs and timely deliveries.[145] In April 2018, Amazon CEO Jeff Bezos announced that Amazon Prime membership exceeded 100 million subscribers globally.[146] These subscribers provide countless amounts of data that Amazon could use to further enhance its healthcare ambitions.[147] The thought of an Amazon health continues to raise concerns with privacy experts who "say the company's increasingly dominant role in our lives raises concerns about how personal data is collected and used," imagine the Alexa in the corner, the shopping lists and wish lists we have created?[148]

These privacy concerns became a reality in healthcare on January 30, 2018, when Amazon announced its joint-venture[149] with global banking institution JP Morgan Chase & Co.[150] and

---

[144] Eric Griffith, *What is Cloud Computing?*, PCMAG (May 3, 2016), https://www.pcmag.com/article2/0,2817,2372163,00.asp.
[145] Farrow, s*upra* note 38.
[146] Dennis Green, *Jeff Bezos finally reveals how many people pay for Amazon Prime*, BUSINESS INSIDER (April 18, 2018), https://www.businessinsider.com/amazon-prime-member-numbers-revealed-2018-4.
[147] *Id.*
[148] *Id.*
[149] Angelica LaVito and Jeff Cox, *Amazon, Berkshire Hathaway, and JP Morgan Chase to partner on US employee health care*, CNBC, (Jan. 30, 2018), https://www.cnbc.com/2018/01/30/amazon-berkshire-hathaway-and-jpmorgan-chase-to-partner-on-us-employee-health-care.html.
[150] "J.P. Morgan is a global leader in financial services." See About Us, J.P. Morgan, https://www.jpmorgan.com/country/US/EN/about (last visited June 25, 2019).

holding company Berkshire Hathaway[151] seeking to transform the healthcare industry by cutting costs and improving quality of care illustrated with Berkshire Hathaway CEO Warren Buffet claiming that "the ballooning costs of healthcare act as a hungry tapeworm on the American economy."[152] The response appears to be mostly positive about the implications Amazon can have on healthcare with industry professionals such as Idris Adjerid–a management information technology professor at the University of Notre Dame–believing that "Amazon in particular can play a strong role if it promotes a greater presence for technological advances including artificial intelligence, and information sharing platforms into health care."[153] But the privacy concerns are monumental for different reasons exhibited by Harvard Law Professor I. Glenn Cohen stating, "Amazon already has huge amounts of our data–we give it to them in exchange for two-day shipping . . . . But what happens when you add in actual health-care data? Many people are already concerned about who has access to that information, and this exacerbates those concerns." [154] Amazon CEO Jeff Bezos

[151] Berkshire Hathaway is a global conglomerate holding company controlling entities such as Geico, Clayton Homes, Duracell, and Dairy Queen. *See Berkshire Hathaway,* http://www.berkshirehathaway.com (last visited June 25, 2019).
[152] LaVito, *supra* note 149.
[153] *Id.*
[154] Abha Bhattarai, *Privacy experts alarmed as Amazon moves into health care industry*, WASHINGTON POST (Jan. 30, 2018), https://www.washingtonpost.com/news/business/wp/2018/01/30/amazon-

acknowledged that "[t]he healthcare system is complex, and we enter into this challenge open-eyed about the degree of difficulty," while JPMorgan Chase CEO Jamie Dimon expressed his belief that "[o]ur people want transparency, knowledge, and control when it comes to managing their healthcare."[155]

The hiring of renowned surgeon Dr. Atul Gawande further illustrates Amazon's desire to enter the healthcare market and make an impact, beginning with improving the care of the workforce of the three companies and expanding from there.[156] The combination of the three companies roughly 1.2 million person workforce[157] plus the global reach of Amazon Prime and other Amazon users, the amounts of customer data that Amazon will have access to raises more concerns than the initial thought may recognize. By organizing their operations together, Amazon will have a global operation with information on individuals ranging from an individual's credit card information, address, family members, prescriptions, weekly deliveries of goods of all types and more. The future of Amazon health is still to be determined, but the use of data is certainly within that future. On

---

already-has-huge-amounts-of-our-data-what-happens-when-you-add-healthcare-to-the-mix/?noredirect=on&utm_term=.fba456b06d67.

[155] LaVito, *supra* note 149.

[156] Angelica LaVito, *Dr. Atul Gawande to start as CEO of Buffett, Bezos and Dimon's health-care venture*, CNBC (July. 9, 2018), https://www.cnbc.com/2018/07/06/dr-atul-gawande-to-start-as-ceo-buffett-bezos-dimon-health-venture.html.

[157] *Id*.

one hand, predictive technology can be used to help improve our personal health and get the individual what is needed, but, on the other, our next side ad could be a medicine that could reveal our most intimate details.

Amazon's cloud service network, AWS, will only further this mission of implementing artificial intelligence and data crunching. Idris Adjerid, while mentioning above[158] his optimism for Amazon's health future, stated, "Amazon is a data-centric company that's good at artificial intelligence and machine learning, so it doesn't take much to see that that's what they'll bring to the health-care industry."[159]

Amazon's entire business model is built upon a foundation of personal data.[160] Professor Galloway, who labeled Amazon as one of his Four Horsemen, writes that "Amazon now offers everything you need, before you need it, delivered in an hour to the 500 million wealthiest households on the planet."[161] This global power and access to data will permit Amazon to expand upon its healthcare ambitions but will it be at the expense of the individual's "private" medical records? Peter Swire, law professor at Georgia Tech University and former White House coordinator

---

[158] LaVito, *supra* note 149.
[159] Bhattarai, *supra* note 154.
[160] Dave Gershgorn, et al., *What is Amazon, really*, QUARTZ (Aug. 20, 2017), https://qz.com/1051814/what-is-amazon-really/.
[161] Galloway, *supra* note 109, at 56.

for HIPAA discussed that "[HIPAA] covers traditional health insurance and provider health care, but it doesn't cover many of the other sources of health-related data that today's technology generates . . . . It doesn't cover, for example, the books you buy about health care or the many fitness and health-care apps you may have on your phone."[162]

ALPHABET'S GOOGLE[163]

Similarly to Amazon's machine learning and cloud based networks, Google is also betting on data configuration and artificial intelligence to make its mark on the healthcare sector.[164] According to a research report by CBInsights,[165] Alphabet is focusing the most attention towards its artificial intelligence capabilities in organizing and interpreting data to provide quicker diagnoses, detect specific trends, and develop disease and lifestyle

---

[162] Bhattarai, *supra* note 154.

[163] Google was originally founded as its search engine but after Google began to spread into other sectors it created Alphabet in 2015 as its parent company that brought under its wing many former Google subsidiaries and Google itself. To promote note clarity, no distinction will be made between the two and mentioning Google will refer the reader to all of its capacities. *See generally* Jillian D'Onfro, *Google is now Alphabet*, BUSINESS INSIDER (Oct. 2, 2015), https://www.businessinsider.com/google-officially-becomes-alphabet-today-2015-10.

[164] Research Report, *How Google Plans To Use AI To Reinvent The $3 Trillion US Healthcare Industry*, CBINSIGHTS, https://www.cbinsights.com/research/report/google-strategy-healthcare/ (last visited January 27, 2019).

[165] CB Insights' machine intelligence platform, intelligence analysts, and global network of executives and startups empower people to articulate compelling answers to difficult questions — about growth, about the competition, and about technology. See generally https://www.cbinsights.com/about. (Author's note).

management.[166] Recent acquisitions have brought Verily and DeepMind, among others, under the Alphabet umbrella of data accumulation.[167] Major focuses for the company following these recent acquisitions include detection and management of eye disease, diabetes, and heart disease.[168] Verily states that they "are running longitudinal studies to better understand ways to predict and prevent disease onset and progression,"[169] while DeepMind focuses broadly on issues ranging "[f]rom climate change to the need for radically improved healthcare, too many problems suffer from painfully slow progress, their complexity overwhelming our ability to find solutions."[170]

For entities that fall within HIPAA's sphere of influence and seek to use Google's cloud network, they "must review and accept Google's Business Associate Agreement," but "[n]ot all Google Cloud products are designed to comply with HIPAA and only specified products are covered under [Google's] Business Associate Agreement."[171] However, one must keep in mind that this is a limited agreement for entities that would like to have their

---

[166] *How Google Plans To Use AI To Reinvent The $3 Trillion Healthcare Industry*, *supra* note 164.
[167] *Id.*
[168] *Id.*
[169] *See Projects*, Verily, https://verily.com/projects/ (last visited June 23, 2019).
[170] *See About Us*, DeepMind, https://deepmind.com/about/ (last visited June 23, 2019).
[171] *See generally Standards, Regulations & Certifications*, Google Cloud, https://cloud.google.com/security/compliance/hipaa-compliance/ (last visited 7/1/2019).

operations maintain compliance with Google products. This does not apply to information that the individual possesses on their own and Google, by simple virtue of it being their product, has access to.

Part III: Enriching Lives While Ensuring Privacy

While Tim Cook states that, privacy is a fundamental human right, and positions Apple as taking what has been traditionally with the institutions and using it to empower the individual, the laws and regulations of the United States and the fifty individual states do not directly support such a notion.[172] The many laws of the United States are vast and overwhelming yet "employ[ ] a 'sectoral' approach to data privacy rather than the 'comprehensive' approach used by jurisdictions such as the European Union."[173] For this reason and due to the potentiality of an individual's medical data being used for improper purposes– such as selling, marketing, profiteering and the like– restructuring must be made in order to credence to the original framework that HIPPA and HITECH established–to ensure the privacy of every individual is guaranteed in the laws and regulations of this country as opposed to the whims of the individual company's executives. As James Madison wrote, "If men were angels, no government

[172] Baum, *supra* note 63.
[173] Nicholas Camillo and Devika Kornbacher, *Example of FIPPS in Current Data Privacy Laws*, 2018 TXCLE Intell. Prop. L. 3-IV, 2018 WL 6186992.

would be necessary." [174] Unfortunately, recent events, from Yahoo[175] and Facebook[176] to the latest fine against Google under the GDPR [177], have vividly demonstrated that an individual's personal data, especially health records, cannot and should not be left to such angelic conditionals.

The protections provided individuals within HIPAA and HITECH will likely cover many operations that the aforementioned companies of Apple, Amazon, and Google will conduct with covered entities, but likelihoods and probabilities are not adequate in a health context when one's health relies upon the accuracy and reliability of such records. However, personal health information that the individual freely provides through platforms such as Apple's Health App and Apple Watch would not fall under HIPAA or HITECH protections unless these companies grow into the definitions provided by the rules or contract with those entities that are. As a result, the United States should adopt a national GDPR Plus[178] framework for healthcare and all such entities that operate within healthcare in order to properly regulate entities such

---

[174] THE FEDERALIST NO. 51, at 322 (James Madison) (Clinton Rossiter ed., 1961).
[175] *Yahoo provides notice to additional users affected by previously disclosed 2013 data theft*, *supra* note 73.
[176] Valdez, *supra* note 74.
[177] Schechner, *supra* note *85.*
[178] This is not recognized terminology but simply a name the author has developed for purposes of this note to analogize to the EU's GDPR law while adding the Plus terminology to designate the link solely to health information and establish the difference between that which is proposed and that of the EU.

as the tech giants while also giving full control to the individual over his or her medical data. As put by Tim Cook in his recent op-ed piece in *Time Magazine*:

> "Meaningful, comprehensive federal privacy legislation should not only aim to put consumers in control of their data, it should also shine a light on actors trafficking in your data behind the scenes
>
> . . . .
>
> We cannot lose sight of the most important constituency: individuals trying to win back their right to privacy. Technology has the potential to keep changing the world for the better, but it will never achieve that potential without the full faith and confidence of the people who use it."[179]

GDPR PLUS FOR HEALTHCARE?

At the outset, this proposition is not meant to be exhaustive, comprehensive, or a full analysis of a potential GDPR Plus option, but rather meant to promote further discussion of this topic and to express the need for proper individual protections. This section will briefly address some overlying concepts to promote future analysis and debate.

In order to fully establish the proposals to follow under GDPR Plus, there will be needed cooperation from the tech giants for further innovation to provide that the individual personally owns his or her medical data as opposed to relying upon the

---

[179] Tim Cook, *You Deserve Privacy Online: Here's How You Could Actually Get It Done*, (Jan. 16, 2019), TIME MAGAZINE, http://time.com/collection/davos-2019/5502591/tim-cook-data-privacy/.

transfer of records from the healthcare provider.[180] If an individual's medical data could all be stored on one's personal device as well as in a personal cloud provider under a system similar to Apple's iCloud Apple ID[181] service or the organ donor heart logo on an individual's driver's license,[182] providers can be certain that the information provided by the individual patient is accurate but more importantly only accessible to those with expressed consent. The implications of the individual possessing his or her own medical data would then require all companies such as the three mentioned above and third party app developers to request an opt-in capability as opposed to an adhesive contractual feel of agree or disagree, all or nothing.

A common argument against such regulation would be that it stifles innovation due to costs being used in order to comply with the regulations instead. Although valid, this contention is misguided because the current framework provides for the ability of fifty states to be creating their own data privacy laws while also

---

[180] Jennifer Shoaf Richardson, *CEOs Lead Charge for National Consumer Privacy Law*, WORKPLACE PRIVACY, DATA MANAGEMENT & SECURITY REPORT (Jan. 17, 2019), https://www.workplaceprivacyreport.com/2019/01/articles/data-security/ceos-lead-charge-for-national-consumer-privacy-law/.

[181] When an individual uses iCloud, the individual uses an email as the username and. Also has a password. Whenever the individual signs into that account on any Apple device, the individual can choose to bring all information present on another device and previously saved. Additionally, the individual may sync all device simultaneously so that information added to one will immediately sync to the other. *See generally* iCloud: What is I ICloud?, Apple (June 20, 2019), https://support.apple.com/kb/PH2608?locale=en_US.

[182] This is essentially an opt-in for your information, tissues and organs to be used to benefit others.

having HIPAA to consider. If a more innovative friendly HIPAA alternative were to be created that would seek to foresee the needed innovation of big tech while also permitting the individual to know the data that is collected and who possessed access to it, the innovation could actually grow exponentially because companies would know their specific parameters and individuals would be safer by knowing what information is out there and who has it.

A main issue with HIPPA and GDPR would be that both prohibit a private right of action, which removes the individual's ability to challenge unless a party were to act on their behalf. Additionally, HIPAA is reactionary not covering new technologies unless they were to partner with the old covered entities and GDPR is too broad covering nearly everything granting too much power to the individual that virtually removes all data that could be used to increase innovation. As a result, a balance should be found between the individual's right and the companies ability to grow and continue to benefit society.

Conclusion

As the big technological powers of Apple, Amazon, and Google continue to innovate and enter the healthcare sector, it would be wise for lawmakers to implement a legal framework to

ensure the protection of an individual's medical data while also embracing further innovation that can benefit the lives of billions across the globe. HIPAA and HITECH were arguably sufficient and perhaps innovative at the turn of the millennium, but the technological advances that have occurred since their inception cry out for an updated framework that connects society's growing concern for privacy in a world of connectedness to society's growing desire to improve our lives and personal health. An opt-in approach would be a good beginning to empower the individual while also preventing the inhibition of innovation that is often the common critique of initial regulatory implementation. The current structure with HIPAA provides for all information to be covered and not transmitted unless specifically designated. This designated approach mirrors a command economy methodology that is resemblant of reactionary additions as opposed to assessing where innovation is going and regulating proactively. Consequently, innovation is often stifled, innocent and or harmless conduct constitute violations, and new developments such as those presented within this note are not covered or present another problem that continues the reactionary cycle approach.

As a result, a uniform system that connects the fifty states under the guidance of a GDPR Plus link would be wise to tackle the inevitably unforeseen consequences that technological

innovation in healthcare can present while also avoiding the multitude of regulatory overlap with the current HIPAA as a floor approach. Although this note does not present by any means an exhaustive analysis or a satisfactory proposal, these questions should be addressed to ensure that society can adjust appropriately to changing circumstances in the future as opposed to reacting radically due to unpreparedness. Technology and healthcare will only become more connected in the future, not less. The future will be what we make it. We best begin making it now.