NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

SECURING HEALTHCARE'S QUANTIFIED-SELF DATA: A COMPARATIVE ANALYSIS VERSUS PERSONAL FINANCIAL ACCOUNT AGGREGATORS BASED ON PORTER'S FIVE FORCES FRAMEWORK FOR COMPETITIVE FORCES

by

Catherine H. Chiang

September 2016

Thesis Advisor: Rodrigo Nieto-Gomez
Co-Advisor: John Rollins

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	September 2016	Master's thesis

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
SECURING HEALTHCARE'S QUANTIFIED-SELF DATA: A COMPARATIVE ANALYSIS VERSUS PERSONAL FINANCIAL ACCOUNT AGGREGATORS BASED ON PORTER'S FIVE FORCES FRAMEWORK FOR COMPETITIVE FORCES	
6. AUTHOR(S) Catherine H. Chiang	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Homeland Security or the U.S. Government. IRB number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT	12b. DISTRIBUTION CODE
Approved for public release. Distribution is unlimited.	

13. ABSTRACT (maximum 200 words)

This thesis explores possible solutions to secure the aggregation and sharing of healthcare's quantified-self data, based on lessons from the personal financial industry. To address this concern, Porter's Five Forces Framework is used to understand how consumers are impacted by the two sectors' differences in legislation, technology, and security. The analysis in this thesis indicates that consumers of financial account aggregators benefit from more secure and interoperable services. In contrast, users of healthcare aggregators are negatively affected by the healthcare industry's higher threat of new entrants and the bargaining power of suppliers. Therefore, healthcare leaders should improve consumer benefits by transforming their industry's competitive forces to mimic those of the financial services industry. To accomplish this goal, industry leaders could focus on filling the gap in the Health Insurance Portability and Accountability Act (HIPAA) for self-generated data, improving security innovations, and attracting third-party developers to secure data interoperability.

14. SUBJECT TERMS	15. NUMBER OF PAGES
quantified-self movement, data aggregation, data sharing, account aggregators, screen scraping, healthcare, personal finance, Porter's Five Forces, competitive forces, information security, privacy, data security and interoperability	107
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

SECURING HEALTHCARE'S QUANTIFIED-SELF DATA: A COMPARATIVE ANALYSIS VERSUS PERSONAL FINANCIAL ACCOUNT AGGREGATORS BASED ON PORTER'S FIVE FORCES FRAMEWORK FOR COMPETITIVE FORCES

Catherine H. Chiang
Management Program Analyst,
United States Citizenship and Immigration Services
B.A., University of California, Berkeley, 2009

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
September 2016**

Approved by: Rodrigo Nieto-Gomez, Ph.D.
Thesis Advisor

John Rollins
Co-Advisor

Erik Dahl, Ph.D.
Associate Chair of Instruction,
Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis explores possible solutions to secure the aggregation and sharing of healthcare's quantified-self data, based on lessons from the personal financial industry. To address this concern, Porter's Five Forces Framework is used to understand how consumers are impacted by the two sectors' differences in legislation, technology, and security. The analysis in this thesis indicates that consumers of financial account aggregators benefit from more secure and interoperable services. In contrast, users of healthcare aggregators are negatively affected by the healthcare industry's higher threat of new entrants the and bargaining power of suppliers. Therefore, healthcare leaders should improve consumer benefits by transforming their industry's competitive forces to mimic those of the financial services industry. To accomplish this goal, industry leaders could focus on filling the gap in the Health Insurance Portability and Accountability Act (HIPAA) for self-generated data, improving security innovations, and attracting third-party developers to secure data interoperability.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

API	Application Programming Interface
APPS	Application Privacy, Protection and Security
BMJ	British Medical Journal
CSV	Common Separated Value
DOW	Dow Jones Industrial Average
EHR	Electronic Health Record
FCRA	Fair Credit Reporting Act
FDA	Food and Drug Administration
FFIEC	Federal Financial Institutions Examination Council
FTC	Federal Trade Commission
GLBA	Gramm-Leach-Bailey Act
HIPAA	Health Insurance Portability and Accountability Act
IEEE	Institute of Electrical and Electronics Engineers
IFTTT	If This Then That
ISO	International Organization for Standardization
PHI	Protected Health Information
PII	Personally Identifiable Information
PIN	Personal Identification Number
PSDO	Partner Standards Development Organization
RIA	Registered Investment Advisors
S&P	Standard and Poors
SDO	Standards Development Organization
SEC	Securities and Exchange Commission
XML	Extensible Markup Language

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

Healthcare industry's quantified-self movement empowers individuals via active self-tracking. This movement describes individuals' use of applications and devices, such as Fitbit, to monitor and manage their health. Most importantly, the granularity of quantified-self data holds the potential to truly personalize healthcare. However, this consolidation of detailed personal data also exponentially increases information security and privacy risks. Ultimately, these vulnerabilities in data aggregation and sharing impede progression towards personalized healthcare. Therefore, this thesis addresses healthcare industry's lack of security with successful practices from the personal financial sector.

To determine applicable smart practices, a comparative case study was conducted between the financial services and healthcare industries. The comparison focused on three key factors that influence data aggregation and sharing in the two sectors: legislation, technology, and security. These areas signify different ways in which industries impact consumer benefits through relevant security and privacy practices. To discern the effects on consumer benefits, this thesis used Porter's Five Forces Framework to evaluate the two sectors. The five forces are competitive rivalry, threat of new entrants, threat of substitute products or services, bargaining power of suppliers, and bargaining power of buyers.[1]

The results of Porter's Five Forces Framework indicate that consumers benefit more from the personal financial industry in comparison to the healthcare sector. The personal financial industry is not as competitive due to its lower threat of new entrants and bargaining power of suppliers. The financial services sector is more resilient to the threat of new entrants, because of its comprehensive legislation and innovative security measures that serve as

[1] Michael E. Porter, *Competitive Strategy: Techniques for Analyzing Industries and Competitors: With a New Introduction* (New York, NY: The Free Press, 1998), http://www.vnseameo.org/ndbmai/CS.pdf.

barriers to entry. Also, since third parties produced most of the financial aggregators, banking institutions have lower bargaining powers as the industry's suppliers. These weaker forces enable personal financial aggregators to provide their consumers with more secure and interoperable services. Therefore, healthcare leaders should reform their industry's competitive forces to imitate that of financial services.

Based on the analysis and outcomes, this thesis provides three recommendations to increase consumer benefits in the healthcare industry. First is to fill the gap in the Health Insurance Portability and Accountability Act (HIPAA). Currently, HIPAA does not define consumers as a covered entity. Hence, its provisions do not protect the security and privacy of user-generated health data. In contrast, policymakers are able to extend financial industry's existing legislation to account aggregators. Thus, users of financial account aggregators continue to enjoy comprehensive protections. To follow suit, policymakers should fill this gap in HIPAA's coverage to ensure the security and privacy of consumer-generated health data.

The second recommendation is to encourage healthcare industry's security innovations. Personal finance as an industry prioritizes its security efforts, as demonstrated by account aggregators' innovative solutions. For example, a leading account aggregator, Mint, has invented and patented its pioneering security process to counter a key vulnerability of the screen scraping aggregation method. Financial account aggregators go to great lengths to reassure their users of information security. This commitment not only deters competitors with sub-standard security measures from entering the market, but it also encourages consumers to adopt account aggregation services. As demonstrated by those in the financial services sector, leaders of the healthcare industry should also focus their efforts on such security innovations.

The last recommendation is to attract third-party developers to facilitate the interoperability of secure data. As producers of most leading financial account aggregators, third-party developers prioritize data integration across

various sources. This focus closely aligns with consumer interests. On the other hand, healthcare corporations assume dominant roles in both manufacturing devices and providing aggregation services. Because of this dual role, corporate leaders tend to be focused solely on the internal interoperability between their devices and the associated apps, rather than external integration with other apps, devices, and platforms. For instance, corporations block public access to their protocols and prevent others from connecting to their devices with proprietary protocols. Moreover, the lack of standardized protocols could result in some databases being more susceptible to hacking, which would cause any connected systems to become vulnerable as well. Therefore, healthcare leaders should moderate corporate ownership to attain secure data integration.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

This thesis could not have become a reality without the consistent guidance and support of many individuals. I am greatly indebted to all of them in addition to the ones mentioned here.

First of all, I would like to recognize the faculty and staff of Naval Postgraduate School's Center for Homeland Defense and Security for providing me with this exceptional opportunity. They have made this program one of my most rewarding experiences.

Specifically, I would like to extend my deepest gratitude to a select few from the school. To my advisors, Rodrigo Nieto-Gomez and John Rollins, thank you for imparting your pivotal insights and for continuing to challenge me throughout this process. Additionally, a special thank you to Nick Drew for your indispensable expertise on Porter's Five Forces Framework. Finally, to Michelle Pagnani and Chloe Woida, I am grateful for your patient coaching in making me a better writer. It has truly been an honor to work with all of you.

Most importantly, I would like to express my utmost appreciation for my family by dedicating this thesis to them. This thesis would not have been possible without their unwavering support and encouragement. Thank you for all that you do.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. RESEARCH QUESTION

As more consumers adopt technologies to quantify their lives, can the healthcare community apply the experience of securing the aggregation and sharing of financial data to the quantified-self data, without discouraging innovation in the healthcare industry?

B. PROBLEM STATEMENT

The quantified-self movement empowers individuals through active self-monitoring. Self-tracking enables participants to quantify their internal and external experiences with the world.[1] As part of the movement, individuals track inputs into the body, emotional and physiological states, and mental and physical performances via wearable technologies.[2] They can immediately observe their bodies' responses to changes in their behaviors, which then motivate them to take ownership of their health.[3] This instant feedback encourages individuals to become more aware and interested in self-monitored health.

Aside from empowering individuals, the quantified-self movement has the potential to truly personalize healthcare. While major advancements in genomic mapping have taken place, tracking of physical indicators such as "blood pressure [and] self-reported activity levels" remains manual and archaic.[4] The quantified-self movement enables the automation of detailed physical and physiological monitoring. Better tracking of these responses would lead to more tailored and effective treatment plans.

---

[1] Nadine Razzouk, "Quantified Self," 2015, http://ft.parsons.edu/skin/wp-content/uploads/2015/05/Nadine_RAZZOUK1.pdf.

[2] Ibid.

[3] Maulik D. Majmudar, Lina Avancini Colucci, and Adam B. Landman, "The Quantified Patient of the Future: Opportunities and Challenges," *Healthcare (Amsterdam, Netherlands)* 3, no. 3 (September 2015): 153–56, doi:10.1016/j.hjdsi.2015.02.001.

[4] Ibid.

Another aspect to accomplishing personalized healthcare is the systematic use of big data analytics. Machine-learning algorithms use databases to produce significant findings.[5] The findings rely on algorithms to establish population-level baselines and to pinpoint variability.[6] Once abnormal behaviors or activities are identified, devices could alert their users with personalized messages. For instance, the optimal hours of sleep a night typically vary from person to person.[7] Therefore, by monitoring an individual's sleep pattern, unusual deviations from the norm could be easily detected. Given Swan's research showing that sleep deprivation and degradation lead to diabetes,[8] a drop in sleep quality could be indicative of serious health conditions that might require behavioral changes. By making individuals aware of such issues, they could then take preventative actions to improve their health.

Along with the aforementioned benefits, the quantified-self movement also exponentially increases the security risks of aggregated and shared information. Traditional personally identifiable information (PII) mainly consists of identity and contact information. Yet, it already carries serious threats to consumers' security and privacy. Posing an even greater threat, self-tracking data captures PII at a much higher volume and greater granularity, which could even be used to predict individuals' future behaviors.[9] Unfortunately, since most self-monitoring services are linked to mobile applications, they retain similar security issues as typical mobile apps.[10] Examples of vulnerabilities include location tracking, unencrypted transmission of personal data, nonexistent privacy policies, contact of multiple

---

[5] Melanie Swan, "The Quantified Self: Fundamental Disruption in Big Data Science and Biological Discovery," *Big Data* 1, no. 2 (June 1, 2013): 85–99, doi:10.1089/big.2012.0002.

[6] Ibid.

[7] Ibid.

[8] Ibid.

[9] Mario Ballano Barcena, Candid Wueest, and Hon Lau, *How Safe Is Your Quantified Self?* (Mountain View, CA: Symantec Corporation, August 11, 2014), 19, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/how-safe-is-your-quantified-self.pdf.

[10] Ibid.

domains, insecure session management, and unintended data leakages.[11] If these vulnerabilities are exploited, malicious actors could use the stolen information for insurance fraud, identity theft, financial gain, prescription drug abuse, or targeted attacks.[12] More importantly, consumers' lives could be seriously threatened if healthcare professionals and researchers used falsified or altered data to derive treatment plans and medical findings. The lack of security would not only sabotage the quantified-self movement, but it could also result in aggressive backlashes from endangered patients.

Ultimately, this lack of security when aggregating and sharing quantified-self data impedes the advancement of personalized healthcare. Leading technology companies are attempting to overcome these barriers via recent application releases. To evaluate the effectiveness and security of the healthcare industry's existing efforts to address this issue, a comparative case study is conducted against successful personal financial aggregators. Specifically, the analysis assesses distinctions between the two industries based on Porter's Five Forces Framework. Smart practices from the financial services are reviewed to offer recommendations for securing the aggregation and sharing of quantified-self data.

C. LITERATURE REVIEW

This literature review focuses on published research regarding data aggregation and sharing in the healthcare and financial industries. The first section describes the aggregation, sharing, and security issues of the quantified-self data. These identified issues are accompanied by respective mitigation strategies. The next section concentrates on the most vulnerable aggregation method in the financial industry, and possible approaches to manage the risks of this method are discussed subsequently.

---

[11] Ibid.

[12] Institute for Critical Infrastructure Technology, "Hacking Healthcare IT in 2016," January 2016, http://icitech.org/wp-content/uploads/2016/01/ICIT-Brief-Hacking-Healthcare-IT-in-20161.pdf.

1. Aggregation, Sharing, and Security Challenges of the Quantified-Self Data

This section examines aggregation, sharing, and security challenges in the healthcare industry along with potential solutions. One of the challenges is data silo, which is driven by corporations that segregate users' information by independently storing it within the bounds of their devices or apps. Secondly, corporate leaders are unwilling to focus their efforts on enabling integration with data from other devices or apps. In addition, users' experiences could be negatively affected by challenges in data quality that stem from duplicate and unverifiable records. Furthermore, quantified-self participants experience increased security and privacy concerns because of the voluminous and frequent accumulation of personal data. The granularity of this data makes protecting individuals' identities even more difficult.

a. Data Silos

Data silos originate from corporations limiting users from accessing their personal data. Since most consumer-generated healthcare data is collected via mobile applications or wearable devices, this data tends to reside within the bounds of service providers. For instance, users' access to minute-to-minute Fitbit data is restricted.[13] To retrieve their data, users need to request special access from the Fitbit team.[14]

The following researchers validate this phenomenon by noting corporate ownership as the primary cause to data fragmentation. As Chris Till states, users' exercise data is compartmentalized and owned by the application or equipment providers.[15] Companies segregate users' data by containing it within their apps

[13] Ernesto Ramirez, "How to Download Minute-by-Minute Fitbit Data," Quantified Self, September 26, 2014, http://quantifiedself.com/2014/09/download-minute-fitbit-data/.

[14] Ibid.

[15] Chris Till, "Exercise as Labour: Quantified Self and the Transformation of Exercise into Labour," *Societies* 4, no. 3 (August 28, 2014): 446–62, doi:10.3390/soc4030446.

or devices, creating barriers to data aggregation.[16] Even though Chris Till's research was based mainly on fitness applications, other researchers support similar findings. Melanie Swan discusses the need to aggregate healthcare information across multiple data streams: "wearable electronics, biosensors, mobile phones, genomic data, and cloud-based services."[17] Overcoming these confinements is the only way to achieve extensive data integration.

Yet, corporate leaders are not producing solutions to eliminate data silos. Shameer et al. pointed out the aforementioned phenomenon of product-specific databases as well as corporations' lack of effort to create integration tools.[18] Without the necessary tools to integrate data, fragmented databases continue to remain isolated. Furthermore, Gay and Leijdekkers indicated that existing protocols are too diverse and not available enough to the public.[19] They also noted that some vendors' proprietary protocols even prevent third parties from communicating directly with the devices. The heterogeneous and inaccessible protocols further obstruct the integration effort.

As one possible solution to integrate data, application programming interface (API) seems to have gained the widest acclaim. API platforms specify how various data sources should interact.[20] Shameer et al. suggest using APIs as a primary method for integration.[21] Also, Gay and Leijdekkers used APIs to create a mobile application, myFitnessCompanion, which integrates activity

---

16 Ibid.

17 Swan, "The Quantified Self."

18 Khader Shameer et al., "Translational Bioinformatics in the Era of Real-Time Biomedical, Healthcare and Wellness Data Streams," *Briefings in Bioinformatics*, February 14, 2016, bbv118, doi:10.1093/bib/bbv118.

19 Valerie Gay and Peter Leijdekkers, "Bringing Health and Fitness Data Together for Connected Health Care: Mobile Apps as Enablers of Interoperability," *Journal of Medical Internet Research* 17, no. 11 (November 18, 2015), doi:10.2196/jmir.5094.

20 Melanie Swan, "Sensor Mania! The internet of Things, Wearable Computing, Objective Metrics, and the Quantified Self 2.0," *Journal of Sensor and Actuator Networks* 1, no. 3 (November 8, 2012): 217–53, doi:10.3390/jsan1030217.

21 Shameer et al., "Translational Bioinformatics in the Era of Real-Time Biomedical, Health Care and Wellness Data Streams."

trackers, wireless sensors, and servers.[22] While this app succeeded in aggregating data from a variety of sources, it is only available for Android platforms and does not integrate with the official electronic health record (EHR) systems, which block all third-party accesses.[23] However, researchers noted existing efforts to integrate APIs, such as Apple HealthKit or ResearchKit, with EHRs.[24] These efforts signify healthcare industry's attempt to close the gap by integrating personal informatics with EHRs.[25] Based on these publications, researchers agree that APIs have the potential to solve the data fragmentation issue, though challenges still exist in integrating personal and EHR data.

b. Data Quality

Once aggregated, data quality could be affected by multiple readings and unverifiable information. In regards to data duplication, Gay and Leijdekkers claim that multiple sources of data could result in numerous recordings, such as simultaneous heart rate readings by different devices.[26] Since different devices might not always capture the same readings, such discrepancies could negatively impact the accuracy of medical research or treatment plans.[27] Subsequently, data reliability is yet another concern, especially since the quantified-self devices are not regulated.[28] Consumers could suffer serious consequences if medical diagnoses are based on unreliable data from inferior sensors.[29]

---

[22] Gay and Leijdekkers, "Bringing Health and Fitness Data Together for Connected Healthcare."

[23] Ibid.

[24] Shameer et al., "Translational Bioinformatics in the Era of Real-Time Biomedical, Healthcare and Wellness Data Streams."

[25] Ibid.

[26] Gay and Leijdekkers, "Bringing Health and Fitness Data Together for Connected Healthcare."

[27] Ibid.

[28] Ibid.

[29] Ibid.

Fortunately, data duplication and reliability issues are manageable. To minimize data discrepancies, apps can allow users to designate the primary source of real-time data.[30] Also, tracking data sources could help to alleviate reliability issues.[31] Consumers, healthcare professionals, and medical researchers could evaluate data quality based on the reliability of its sources. These straightforward solutions for data duplication and reliability can be easily implemented to improve information quality.

c. Privacy and Security

In addition to data interoperability and quality concerns, quantified-self participants do not want their privacy compromised in exchange for sharing their information. A 2014 *American Health Information Management Association Journal* article indicated that over 90% of those willing to share their data prioritized the need for anonymity.[32] These consumers believe in advancing healthcare by sharing detailed information about their behaviors, but they insist on maintaining their privacy. According to Diamond et al., privacy is a key attribute in obtaining public trust for information sharing.[33] Anonymity drives voluntary participation, which increases the volume and accuracy of data available for medical diagnoses and research studies.

Notably, privacy is especially important to consumers when sharing their information with the government. Anderson et al. claim that consumers require additional assurance to share information with the government and public health agencies versus hospitals and pharmaceutical companies.[34] However, traditional

---

[30] Ibid.

[31] Ibid.

[32] Harry Rhodes, "Accessing and Using Data from Wearable Fitness Devices" 85, no. 9 (September 2014): 48–50.

[33] Carol C. Diamond, Farzad Mostashari, and Clay Shirky, "Collecting And Sharing Data For Population Health: A New Paradigm," *Health Affairs* 28, no. 2 (March 1, 2009): 454–66, doi:10.1377/hlthaff.28.2.454.

[34] Catherine L. Anderson and Ritu Agarwal, "The Digitization of Healthcare: Boundary Risks, Emotion, and Consumer Willingness to Disclose Personal Health Information," *Information Systems Research*, April 8, 2011, http://pubsonline.informs.org/doi/abs/10.1287/isre.1100.0335.

mechanisms to ensure data privacy, such as HIPAA, need to be revamped to match the current capabilities of data sharing via social networks and other means.[35] Rhodes believes that as the industry reaches a level of maturity, information standardization and governance will be addressed accordingly, along with the need to balance privacy, confidentiality, security, intellectual property, and science.[36]

Despite the emphasis on privacy, risks of compromising consumers' identities surge, because detailed personal data is gathered and shared at a high frequency. Swan argues for difficulty in protecting individuals' identities when a large quantity of personal healthcare data is openly shared.[37] This dataset allows patterns of distinctive characteristics to be tracked. As more behaviors are digitized, these unique characteristics could easily be used to identify individuals.

Apart from privacy, real-life implications of these data also support the need for enhanced security. Swan predicted that data would become an intermediary of individuals' experiences with reality, and thereby taking on a more intimate role.[38] Swan continued to suggest that it would become an extension of people's subjective experiences with the potential to change behaviors. In essence, individuals' experiences are translated into a sequence of numbers. After assessing these values, individuals could adjust how they interact with their surroundings accordingly. Therefore, they could gravely endanger their health if they modified their behaviors based on tampered data. This intimate relationship with the quantified-self data would require more robust security to prevent malicious manipulation.

As a result, possible solutions have been suggested to boost the security of quantified-self data. Based on a white paper published in 2014, Symantec

[35] Swan, "Sensor Mania! The internet of Things, Wearable Computing, Objective Metrics, and the Quantified Self 2.0."

[36] Harry Rhodes, "Accessing and Using Data from Wearable Fitness Devices."

[37] Swan, "Sensor Mania! The internet of Things, Wearable Computing, Objective Metrics, and the Quantified Self 2.0."

[38] Swan, "The Quantified Self."

Corporation described various security issues with the quantified-self movement and provided possible mitigation strategies for using a single data stream.[39] Symantec's recommendations for users include effective passwords, device-based security measures, full device encryption, and disabling Bluetooth whenever possible. Even though Symantec only focused on vulnerabilities of one data source, it identified risks and solutions that could be applicable to aggregated data as well. On the other hand, Doukas et al. support digital certificates and PKI data encryption to secure the internet of Things gateways that aggregate health data from sensors.[40] Their solutions warrant that patients' data are shared securely with authenticated recipients. As a third option, Diamond et al. claim that collecting only aggregated data will mitigate concerns regarding centralized databases of PIIs.[41] Preventing aggregators from collecting PIIs from start removes any traceability to the participants. Thus, far, despite consensus to prioritize security, researchers have yet to reach an agreement on the best solution to address these challenges.

2. The Most Vulnerable Method of Financial Account Aggregation

Financial account aggregators, like Mint, have succeeded in advancing the security of personal financial services. These web services provide individuals a holistic view of their financial portfolios with ease and security. Despite concerns, none of the financial aggregators in the United States are authorized to transfer funds as of 2002.[42] Without the potential risk of compromising users' bank accounts, financial aggregators continue to flourish.

---

[39] See Barcena, Wueest, and Lau, *How Safe Is Your Quantified Self?"*

[40] C. Doukas et al., "Enabling Data Protection through PKI Encryption in IoT M-Health Devices," in *2012 IEEE 12th International Conference on Bioinformatics Bioengineering (BIBE)*, 2012, 25–29, doi:10.1109/BIBE.2012.6399701.

[41] Diamond, Mostashari, and Shirky, "Collecting And Sharing Data For Population Health."

[42] Hiroshi Fujii et al., "E-Aggregation: The Present and Future of Online Financial Services in Asia-Pacific," SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, July 1, 2002), http://papers.ssrn.com/abstract=376864.

There are three main methods of account aggregation: screen scraping, permissive aggregation, and user-driven aggregation. Screen scraping requires an individual's authentic username and personal identification number (PIN) for each bank account in order for the aggregator to obtain user's information from these accounts.[43] Permissive aggregation, or direct feed, describes the method of partnering with financial institutions to obtain direct access to users' accounts.[44] The third method, user-driven, requires users to download agent software onto their personal computers.[45] Then, aggregator services can access users' accounts via the authentications stored on users' computers.[46] Given that screen scraping is the most popular yet least secure method of the three, the subsequent sections primarily focus on exploring its weaknesses and the financial industry's responses.

a. Vulnerabilities of Screen Scraping

The screen scraping method is accompanied by three main vulnerabilities. The Federal Financial Institutions Examination Council (FFIEC) warned against screen scraping because of its associated weaknesses.[47] First is the need to surrender users' login information to the account aggregators.[48] By surrendering their account access information, consumers amplify the risk of their accounts being compromised. Delivery of accurate data is another concern, since frequent updates to banks' websites could result in unreliable data.[49] Screen scraping requires very specific mapping to websites' layouts, so any changes to the

---

[43] Manish Agrawal et al., "A Conceptual Approach to Information Security in Financial Account Aggregation," in *Proceedings of the 6th International Conference on Electronic Commerce*, ICEC '04 (New York, NY: ACM, 2004), 619–26, doi:10.1145/1052220.1052299.

[44] Ibid.

[45] Ibid.

[46] Ibid.

[47] FFIEC, "FFIEC IT Examination Handbook InfoBase – Appendix D: Aggregation Services," accessed January 22, 2016, http://ithandbook.ffiec.gov/it-booklets/e-banking/appendix-d-aggregation-services.aspx.

[48] Ibid.

[49] Ibid.

websites would directly impact data quality. Also, these aggregators need to proactively seek out and capture new information, because they are not synchronized with users' bank accounts for automatic updates. As a result, the aggregation services might not always display the most current account data. Third is users' dependency on aggregators' ability to protect their usernames and passwords.[50] This vulnerability poses the greatest threat to information security. Ann Spiotto confirmed that screen scraping is the most popular yet dangerous method, because of its possible data errors, delays in transmission, and security issues relating to the use of consumers' usernames and PINs.[51] In essence, screen scraping is vulnerable predominantly because it requires users to surrender their bank accounts' logon information.

In contrast to screen scraping, user-driven agent and direct feed are perceived to be more secure because neither requires users to surrender their account information. For user-driven agent software, Agrawal et al. indicated that this alternative was introduced solely due to strong security concerns regarding screen scraping.[52] They also stated that the user-driven method is perceived to be more secure, because it does not require users to surrender their account logon information. In regards to direct feed, FFIEC reasoned it to be a more reliable and traceable method compared to screen scraping.[53] Despite FFIEC's preference for direct feed, this method relies heavily on the partnership between aggregators and financial institutions, thus making it more difficult to pursue.

b. Suggested Solutions

Since screen scraping is unlikely to be completely replaced, researchers have suggested solutions to relief some of its core vulnerabilities. Agrawal et al.

---

[50] Ibid.

[51] Ann S. Spiotto, "Financial Account Aggregation: The Liability Perspective," *Fordham Journal of Corporate & Financial Law* 8, no. 2 (2003): 557–605.

[52] Agrawal et al., "A Conceptual Approach to Information Security in Financial Account Aggregation."

[53] FFIEC, "FFIEC IT Examination Handbook InfoBase – Appendix D: Aggregation Services."

stated that the primary issue is that banks are unable to differentiate users' identities.[54] Since consumers and aggregators currently share the same credential, accesses from these two parties are indistinguishable to financial institutions.[55] To manage this issue, proposed options include two-password model and logon pattern.[56] The two-password model recommends for banks to issue different passwords to users and aggregators.[57] On the other hand, the logon pattern detection distinguishes the two groups by identifying aggregators' automatic logon and logoff patterns versus that of consumers' manual logons.[58]

Conversely, banks could reduce security and privacy concerns by taking on an active role in managing account aggregators. The Office of the Comptroller of the Currency of the Administrator of National Banks published a news release in 2001 for the Second Account Aggregation Conference to persuade firms to become an aggregator rather than being aggregated.[59] Banks can successfully assume the aggregator role by overseeing their relationships with third parties and taking on responsibilities to ensure customer privacy.[60] Moreover, as noted by Ann Spiotto,[61] banks' concerns diminished when they tried to partner with aggregator entities.

Yet even with notable vulnerabilities associated with screen scraping, industry leaders refused unnecessary regulations that would hinder technological progression. Spiotto believes it made more sense to let businesses develop

---

54 Agrawal et al., "A Conceptual Approach to Information Security in Financial Account Aggregation."

55 Ibid.

56 Ibid.

57 Ibid.

58 Ibid.

59 Julie L. Williams, "The Impact of Aggregation on the Financial Services Industry" (Second Account Aggregation Conference, Tysons Corner, Virginia: Administrator of National Banks, 2001), 1–7, http://www.occ.gov/static/news-issuances/news-releases/2001/nr-occ-2001-39.pdf.

60 Ibid.

61 Ann S. Spiotto, "Financial Account Aggregation: The Liability Perspective."

before taking actions out of fear for liability.[62] Furthermore, a number of correspondents argued against regulations that might prevent the creation of innovative solutions that benefit consumers.[63] Since existing laws do protect users of aggregation services from financial losses, there is no immediate need for new regulations until the current ones become insufficient. Most importantly, developers of account aggregators have not declared any security breaches due to vulnerabilities of screen scraping.

3. Conclusion

This literature review demonstrates that there are some areas of consensus as well as some gaps in existing research for the healthcare sector. Currently, quantified-self participants are concerned about their information security and privacy, because of the vast and detailed data collected via healthcare aggregators. However, researchers have not presented consistent solutions. Therefore, given its success in securing the most vulnerable method of data aggregation, the personal financial industry might be able to provide some insights into how healthcare leaders could address securing the aggregation and sharing of quantified-self data.

D. RESEARCH DESIGN

The following sections discuss the study design. The sections include research objective, sample selection, data sources, method, and expected outcomes. To address the research question, this thesis focuses on a comparative study between the personal financial and healthcare industries. The comparison is expected to yield recommendations for healthcare leaders and policymakers.

---

62 Julie L. Williams, “The Impact of Aggregation on the Financial Services Industry.”

63 Ibid.

1. Objective

The objective of this thesis is to obtain best security and privacy practices from the financial sector to apply to the healthcare industry. As an industry, personal finance has had a history of experience and success in digital information security. On the other hand, the healthcare sector has just started to embark on this journey of building its digital database via the quantified-self movement. Therefore, personal financial industry's smart practices would help to expedite healthcare sector's efforts in overcoming relevant security and privacy concerns in order to achieve personalized healthcare.

2. Sample Selection

To compare the two industries, three factors are selected to demonstrate how each sector relates to its consumers. The factors are legislation, technology, and security. These elements represent the different ways that consumers could be impacted by industries' practices. For legislation, this thesis examines existing laws and regulations relevant to data aggregation and sharing. In terms of technology and security, the functionalities of selected aggregators are assessed with respect to each factor.

The aggregators are selected based on their relevance, amount of publically available information, industry dominance, and distinguishing functionalities. For financial services, Mint (owned by Intuit) and Personal Capital (owned by Yodlee) are used as primary examples given the two services' reputations, longevity, and popularity among their users. These two services not only represent the most established financial aggregators, but both are also supported by reputable financial software companies. Additionally, Betterment is included for its innovative investments tools.

With the same selection criteria, aggregators developed by Apple and Google are included as predominant examples from the healthcare industry. The specific applications and APIs are Apple Health, HealthKit, ResearchKit, CareKit,

and Google Fit. Lastly, Sherbit, a newly released application, is also studied for its promising capabilities to advance the quantified health.

3. Source Data

This thesis is supported mainly by qualitative data. Data sources include journal articles, research papers, government publications, news reports, and reviews and specifications of apps and APIs. These qualitative data are obtained via online resources such as government websites, Google Scholar, professional associations, Wall Street Journal, Apple, Google, Yodlee, and Intuit. Relevant information from these sources is presented to compare the two industries' current security measures. It is also used subsequently to determine healthcare sector's areas of improvement.

4. Method

From the policymakers' perspective, consumer benefits and protections are of the utmost importance. To understand how different industry's dynamics impact consumer benefits, a comparative analysis is conducted based on Porter's Five Forces Framework. First, an overview of each industry is provided, comprising of the aforementioned categories: legislation, technology, and security. Then, to assess how the two industries relate to their consumers, each of the five forces is used as a basis for comparison. Finally, factors contributing to the success of financial account aggregators are evaluated to determine best practices that could be reapplied to the healthcare industry.

5. Outcome

The finished product consists of recommendations to secure healthcare data based on lessons from the financial services. Healthcare leaders could use the outputs from this thesis to better secure the aggregation and sharing of the quantified-self data. As a result, the recommended changes would help to build bigger and more robust databases that benefit the consumers, medical researchers, and healthcare professionals. Additionally, policymakers could

formalize the recommendations as policies or legislations to further safeguard consumers' information security and privacy.

II. PERSONAL FINANCE

Traditionally, financial transactions required the tangible movement of money and involvement of brick-and-mortar institutions. Money is a medium of exchange and is used to trade for goods or services.[64] Common forms of money included precious metals, paper currency, and even paper receipts, such as checks.[65] The trading of money is recorded as a financial transaction.[66] Payment from one party to another represented the transferring of wealth ownership. For the transaction to take place, individuals needed to physically enter a bank and withdraw money, which are then handed or mailed to the receiving party.[67] The other option is via the exchange of personal checks, which the recipient would then take to the bank to trade for money.[68]

In contrast, financial transactions today are digitized with the evolution of electronic money and internet finance. Electronic money "exists only in banking computer systems and not held in any physical form."[69] In essence, it is virtual money represented by numbers transmitted from banks to customers.[70] The widespread adoption of digital currency enabled the development of electronic finance as a new channel to deliver financial management services.[71] Electronic finance is the use of digital communication and computation to provide financial

---

64 David Wessel, "The Hutchins Center Explains: How Blockchain Could Change the Financial System (part 1)," *The Brookings Institution*, accessed June 4, 2016, http://www.brookings.edu/blogs/up-front/posts/2016/01/11-how-blockchain-change-financial-wessel.

65 Ibid.

66 Ibid.

67 NBC News, "What It Was Like Before ATMs and Online Banking," NBC News, accessed June 4, 2016, http://www.nbcnews.com/video/what-it-was-like-before-atms-and-online-banking-472991811754.

68 Ibid.

69 F. Sameni Keivani, M. Joubarkand, and M. Khodadadi, "A General View on E-Banking" (Roudsar, Iran: Department Accounting, Islamic Azad University, Roudsar and Amlash Branch, n.d.).

70 Ibid.

71 Ibid.

services.[72] These services include online banking, electronic fund transfers, and investments.

Given the growth of internet-based services, financial account aggregators are developed to fill the gap of convenience and efficiency. Typically, an individual have accounts with several organizations. In order to obtain an overview of his or her financial standing, the individual needs to log into each account separately and manually assemble each piece of their financial puzzle. This tedious process can be replaced by adopting an account aggregator. An account aggregator is an entity that collects "financial information transparently from multiple sources and analyzes it."[73] Account aggregation allows for the convergence of personal financial data. This automated service eliminates the need for consumers to manually gather their financial information from multiple accounts.

Another added benefit, account aggregators empower individuals by providing insights into their financial data. The shift towards electronic finance forces institutions to focus on providing exceptional customer services tailored to the diverse needs of multiple customer segments.[74] To meet these needs, account aggregators deliver personalized financial planning advices with respect to saving, spending, and investing wealth.[75] Aggregators do not simply combine data from various financial accounts. These services recommend behavioral changes to support users in reaching their financial goals.[76]

Aside from benefiting the consumers, transactional data helps lending institutions with managing credit risks. Typical risk estimates are based on limited

---

[72] Ibid.

[73] Fujii et al., "E-Aggregation."

[74] Kate Stalter, "The Future of Banking," accessed June 4, 2016, http://money.usnews.com/money/personal-finance/articles/2015/06/29/the-future-of-banking.

[75] Ibid.

[76] Philip Moeller, "How to Track All Your Money From One Place," U.S. *News & World Report*, May 24, 2013, http://money.usnews.com/money/blogs/the-best-life/2013/05/24/how-to-track-all-your-money-from-one-place.

information from the credit bureaus. The use of transactional data projects a much more comprehensive overview of a person or a company's financial health.[77] For instance, the amount of taxes a business pays can indicate its profitability.[78] Furthermore, transactional data could help peer-to-peer lenders to more accurately differentiate between high and low credit-risk investments and appropriately balance risks across their portfolio.[79]

Finally, everyone benefits from the sharing of aggregated data. In 2010, Mint had delivered a public real-time economic index that drilled down to the city level (Figure 1).[80] This index was calculated based on aggregated transactional data from the anonymous two million of Mint's thirteen million users, who opted to participate in this program.[81] Participants could compare their spending habits to others in the vicinity, or even nationally, to gain insights into how their peers are budgeting.[82] In turn, this targeted information help consumers to adjust their spending decisions accordingly. Additionally, researchers and policymakers could use this index to evaluate real-time economic impacts of policies, global events, and natural disasters.

[77] The Economist, "Cracking the Vault," *The Economist*, October 24, 2015, http://www.economist.com/news/finance-and-economics/21676826-grip-banks-have-over-their-customers-weakening-cracking-vault.

[78] Ibid.

[79] Ibid.

[80] BusinessWire, "What Do People Really Spend? Mint Data Delivers Real-Time View," October 28, 2010, http://www.businesswire.com/news/home/20101028005921/en.

[81] Luke Landes, "Mint.com Tracks Two Million Users to Create Spending Index," accessed June 11, 2016, http://www.consumerismcommentary.com/mint-intuit-consumer-spending-index/.

[82] Ibid.

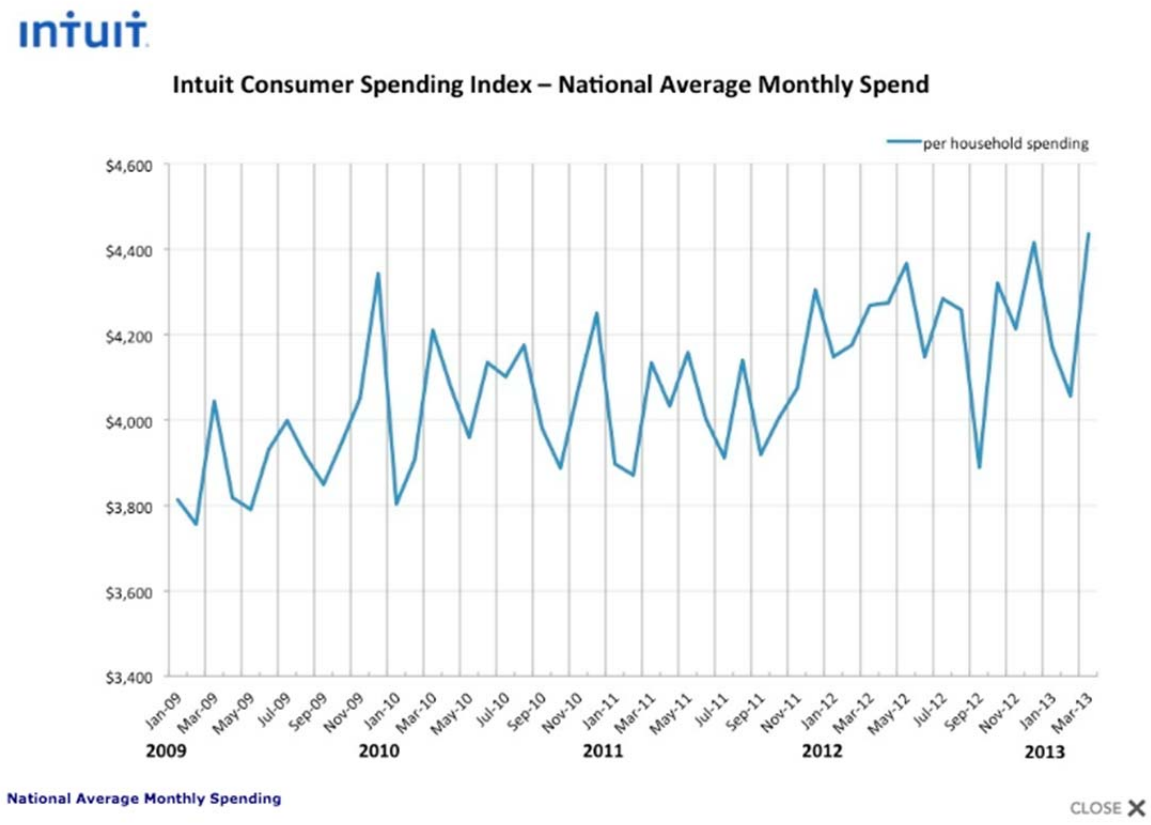

Figure 1. Consumer Spending Index from Mint.[83]

In order to reap the aforementioned benefits, the following sections examine three key factors that greatly contributed to the flourishing industry. These key elements are legislation, technology, and security. Legislations and regulations protect consumer benefits. On the other hand, the accompanying technology defines purpose and encourages consumer adoption. Lastly, information security and privacy are imperative to ensure growing participation.

A. LEGISLATIONS AND REGULATIONS

The rise of electronic finance's popularity urges scrutiny of applicable legislations and regulations. Online financing did not exist prior to the enactment of some of the laws regulating financial services. Therefore, understanding how

[83] Source: Ibid.

policymakers applied existing legislations to new services will be insightful, since their decisions directly impact the growth of an industry.

In regards to security and customer liability, the Federal Reserve Board still has yet to issue clear guidance on the applicability of Regulation E. Enacted in 1978, Regulation E defines a financial institution as one which issues its customers "an 'access device' (such as an ATM and PIN)" and allows electronic funds transfer.[84] This regulation limits customer liability and holds institutions responsible for customers' losses due to security breaches.[85] Federal Reserve Board has sought comments from the public regarding the applicability of Regulation E to account aggregators, but it has yet to issue formal clarifications after the comment period had ended on August 31, 2000.[86] However, the regulation does include language indicating that those services not explicitly stated in the regulation would fall under Federal Trade Commission's (FTC) jurisdiction.[87] Additionally, the Office of the Comptroller of the Currency of the U.S. Department of the Treasury issued guidance in February 2001 to encourage banking institutions to take on a more conservative interpretation if they choose to provide account aggregation services.[88] However, the guidance referred strictly to banks interested in providing aggregation services. Independent or external aggregators were not explicitly mentioned.

Conversely, the Gramm-Leach-Bailey Act (GLBA) clearly describes confidentiality safeguards for consumers using account aggregation services. The GLBA defined financial institutions as any organization that engages in financial activities, such as data processing, transmission, hardware, and

---

84 John Hackett, "Domesticating Account Aggregators," Bank Technology News, accessed June 5, 2016, http://www.americanbanker.com/btn/13_10/-135131-1.html.

85 Ibid.

86 Ibid.

87 Ibid.

88 Office of the Comptroller of the Currency, "Bank-Provided Account Aggregation Services: Guidance to Banks," February 28, 2001, http://www.occ.gov/news-issuances/bulletins/2001/bulletin-2001-12.html.

software.[89] Thus, the FTC and Federal Reserve Board interpreted GLBA privacy provisions to include account aggregators.[90] The privacy requirements, Title V of the GLBA, require written policies and disclosures to customers.[91] Also, account aggregators need to allow customers to opt out of sharing information with non-affiliates, and they could only share aggregated information with third parties to support their services.[92] These requirements protect information confidentiality and empower consumers with control over their shared data.

Another possible privacy trigger is the Fair Credit Reporting Act (FCRA). The FCRA regulates consumer reporting agencies, which are institutions that share customers' information gathered outside of their businesses or services.[93] FCRA considers the disclosing organization a consumer reporting agency, unless the receiving party is an affiliate and complies with providing FCRA notification and opt-out provisions.[94] If dictated as a consumer reporting agency, the institution must "ensure that the information it provides will be used for legitimate business purposes, to maintain the integrity of the data, and to provide notice to consumers of their ability to review and correct inaccurate information."[95] These mandates warrant the accuracy and quality of data being disseminated about the consumers. Applicability of FCRA to account aggregators will depend on organizations' data gathering and sharing practices.

Despite having the necessary legislations and regulations in place, none overtly refers to account aggregators. While GLBA is the most clearly interpreted,

---

89 Kimberly Wierzel, "If You Can't Beat Them, Join Them: Dara Aggregators and Financial Institutions," *North Carolina Banking Institute* 5, no. 1 (April 1, 2001): 457.

90 Ibid.

91 Ibid.

92 Heidi Mandanis Schooner and Michael Taylor, "United Kingdom and United States Reponses to the Regulatory Challenges of Modern Financial Markets," *Texas International Law Journal* 38 (2003): 317.

93 Office of the Comptroller of the Currency, "Bank-Provided Account Aggregation Services."

94 Ibid.

95 Marc S. Roth and Charles Washburn, "Data Brokers Face Blurring Lines, Increased Regulatory Risks," accessed June 5, 2016, http://www.bna.com/data-brokers-face-blurring-lines/.

Regulation E and FCRA are still left open for interpretation. This level of flexibility seems to display an encouraging attitude towards the advancement of account aggregators.

B. TECHNOLOGY

Account aggregators typically use the screen scraping method to gather users' information. Screen scraping "involves the simulation of users' behaviors to access the financial account website and scrape account summary information from the site."[96] Essentially, an aggregator logs into users' accounts with their logon information. Then, the aggregator extracts data from accounts' webpages and consolidates them in one central location. Financial aggregators automate this process as well as summarize and analyze users' account information. The following two sections examine the most notable aggregation and sharing features of personal financial aggregators.

1. Data Aggregation

Account aggregators motivate individuals to become their own financial managers with real-time, simple, and insightful dashboards. Delivering a centralized hub, Mint automatically gathers real-time information from users' bank accounts, credit bureaus, and investment companies.[97] The Intuit supported software saves users the time and effort involved in logging onto various financial accounts to collect up-to-date budget information. Its interface provides an overview of users' financial health at a glance. In one screen, Mint displays wealth allocation across various accounts as well as trends, alerts, credit score, and personalized advices (Figure 2).[98] Along with the overview, Mint provides additional tabs showing users' transactions, goals, trends, investments

[96] Ann S. Spiotto, "Financial Account Aggregation: The Liability Perspective."

[97] Mint, "All in One," Mint, accessed February 21, 2016, https://www.mint.com/.

[98] Johanna Scott, "New Integration with Mint," Betterment, November 16, 2011, https://www.betterment.com/resources/inside-betterment/new-integration-with-mint/.

and ways to save. Users can get a current and complete picture of their net worth at any time and on any device.

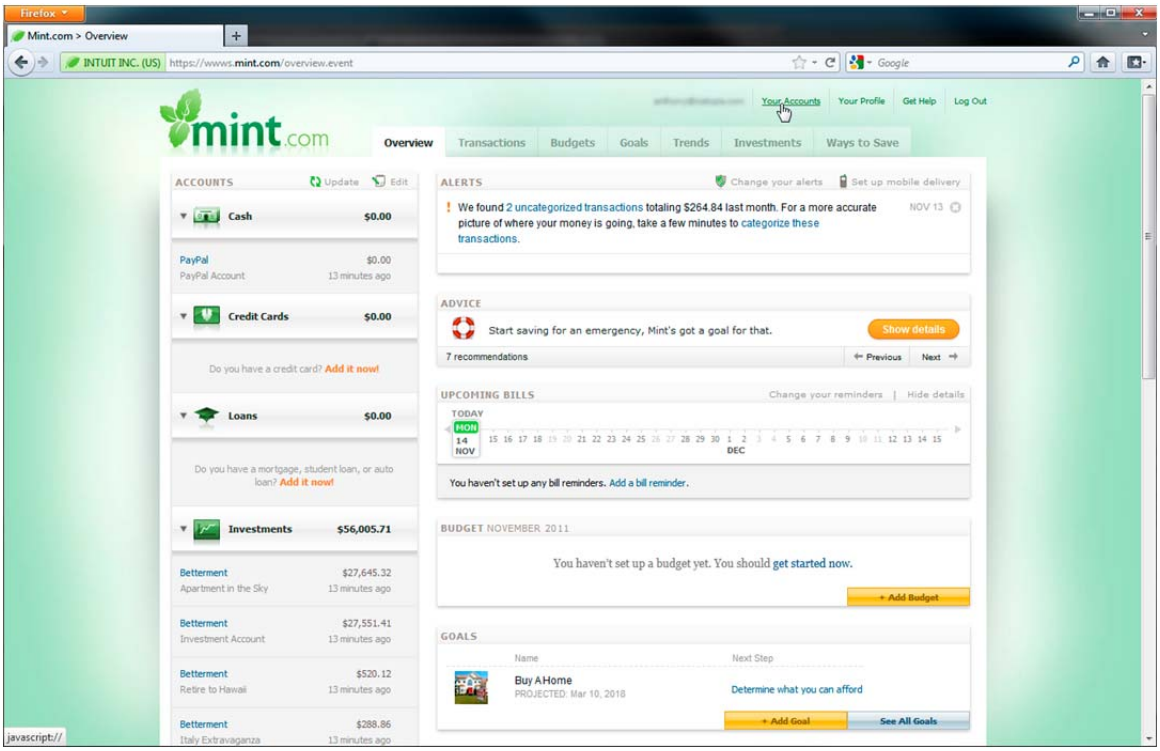

Figure 2. Dashboard of Mint.[99]

Proactive monitoring is another key feature of account aggregators. Mint is capable of providing up to twenty types of alerts for its users.[100] These warnings include notifications of over budget, hidden fees, suspicious account activities, and bill reminders.[101] Mint signals areas requiring additional attention and alleviate hidden financial burdens from unsuspecting customers. With financial aggregators, users can now be alerted of any issue regarding their accounts, whereas these anomalies might have gone undetected otherwise.

---

[99] Source: Ibid.

[100] Mint, "All in One."

[101] Ibid.

Furthermore, automated adjustments reduce the need for users to make changes manually. Betterment manages users' investments based on their financial goals. As a robo-advisor, it uses digital algorithms to optimize its portfolio analysis and investment strategies.[102] Focused on investing for retirement funds, Betterment tends to maximize return with minimal risks.[103] It automates users' retirement planning with its proprietary tools, such as auto-deposits, SmartDeposit, and intelligent account rebalancing.[104]

Aside from managing current expenditures and investments, financial aggregators allow users to anticipate and adapt to life-changing events. Personal Capital provides tailored portfolio management with a synopsis of personal net worth, portfolio analysis, and retirement planner (Figure 3).[105] Via analytics, Personal Capital let users see how planned or unplanned events impact their financial health. Specifically, users could experiment and evaluate how certain events affect their retirement goals.[106] These events include college tuitions, purchase of a new home, marriage, and adoption.[107] This feature prepares users for possible adjustments they might need to make in order to accommodate these life events without diverting from their financial goals.

---

[102] Betterment, "Why Betterment," Betterment, accessed May 30, 2016, https://www.betterment.com/why-betterment/.

[103] Ibid.

[104] Ibid.

[105] Personal Capital, "Free Finance Tools, Calculators & Software," accessed April 14, 2016, https://www.personalcapital.com.

[106] Ibid.

[107] Ibid.

Figure 3. Retirement Planner from Personal Capital.[108]

Lastly, users can compare their overall financial standing to the market. Personal Capital allows users to compare their indexed rate of return to that of the stock market (Figure 4).[109] Market trends available for comparison include the Standard and Poors (S&P) 500, Dow Jones Industrial Average (DOW), Foreign Index, and U.S. Bond Index.[110] The graph visualizes users' portfolio performances against that of the market. Users could use this function as an additional tool to evaluate the growth of their investments with considerations for market conditions.

[108] Source: Ibid.

[109] Kristin Wong, "How to Start Tracking Your Investments With Personal Capital," *Two Cents*, accessed May 30, 2016, http://twocents.lifehacker.com/how-to-start-tracking-your-investments-with-personal-ca-1697801188.

[110] Ibid.

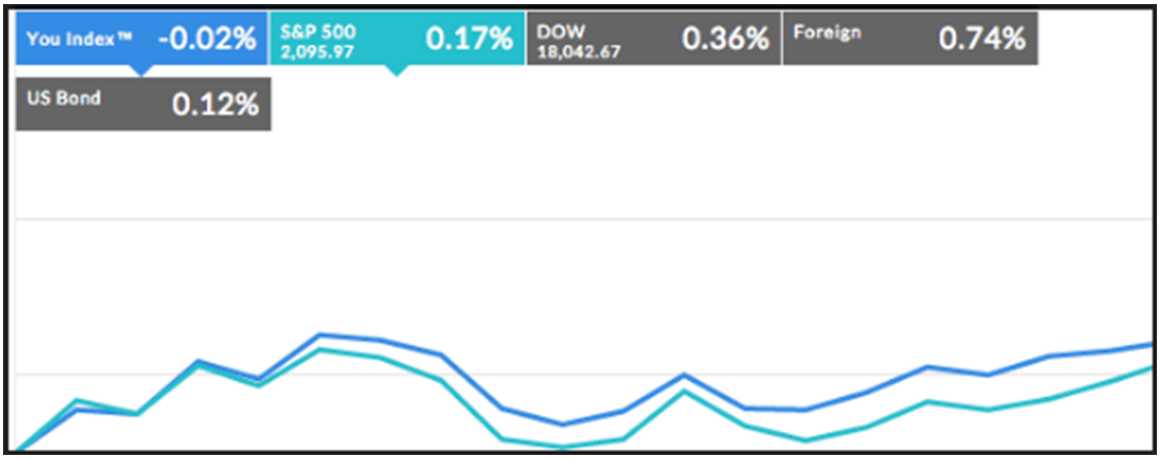

Figure 4. Graph of Market Trend Comparison from Personal Capital.[111]

2. Data Sharing

Users can obtain their financial data from account aggregators. Transactional data from Mint can be exported as a common separated value (CSV) file (Figure 5).[112] Users are then able to share this raw data or perform any additional analysis to their liking. Mint empowers users by providing them the option to access, share, and own their aggregated financial data.

[111] Source: Ibid.

[112] Emily Price, "10 Things You Didn't Know Mint Could Do," Mashable, accessed April 15, 2016, http://mashable.com/2012/08/22/mint-tips/.

	A	B	C	D	E	F	G	H	I
1	Date	Descriptic	Original D	Amount	Transactic	Category	Account N	Labels	Notes
2	9/19/2014	Pennsylva	PENNSYLV	47.68	debit	Utilities	CHECKING		
3	9/12/2014	UGI Utiliti	UGI-UTILI	24.39	debit	Utilities	CHECKING		
4	9/9/2014	FirstEnerg	FIRSTENEF	133.13	debit	Utilities	CHECKING		
5	8/20/2014	Pennsylva	PENNSYLV	53.81	debit	Utilities	CHECKING		
6	8/13/2014	UGI Utiliti	UGI-UTILI	21.4	debit	Utilities	CHECKING		
7	8/6/2014	FirstEnerg	FIRSTENEF	80.46	debit	Utilities	CHECKING		
8	7/21/2014	Pennsylva	PENNSYLV	50.75	debit	Utilities	CHECKING		
9	7/15/2014	UGI Utiliti	UGI-UTILI	24.39	debit	Utilities	CHECKING		
10	7/9/2014	FirstEnerg	FIRSTENEF	128.96	debit	Utilities	CHECKING		

Figure 5. Exportable CSV File from Mint.[113]

Moreover, account aggregators allow users to designate an additional party to be informed. Mint's weekly summaries are "built for two."[114] Users can elect to have a partner to also receive account updates. Correspondingly, Betterment provides the option for joint accounts.[115] This option allows both account holders to create common goals, transfer funds, change allocations, and monitor the account.

Aside from sharing information with friends and family, personal financial aggregators connect users to professional advisors as well. Users of Personal Capital have access to dedicated advisors to help them create a "globally diversified investment portfolio tailored around…[their] unique financial goals."[116] These advisors are Registered Investment Advisors (RIA), legally bound act in the clients' best interests.[117] Access to financial expertise can be done remotely or in-person.[118] Personal Capital provides a hybrid model of technologically

[113] Source: Imgur, "Imgur: The Most Awesome Images on the Internet," Imgur, accessed June 12, 2016, http://imgur.com/TbSKGAl.

[114] Price, "10 Things You Didn't Know Mint Could Do."

[115] Betterment, "Betterment Joint Accounts," accessed June 12, 2016, http://support.betterment.com/customer/portal/topics/749330-joint-accounts.

[116] Personal Capital, "Free Finance Tools, Calculators & Software."

[117] Ibid.

[118] Ibid.

enhanced advising, combining both robo-advising and dedicated financial advisors.

C. SECURITY

Despite the technological benefits of screen scraping, its associated risks need to be examined as well. As the most convenient method of account aggregation, screen scraping is also the most vulnerable. Therefore, it would be invaluable to review some of the personal financial industry's countermeasures. The following sections explore security practices implemented by developers of financial aggregators.

1. Data Aggregation

Developers of financial account aggregators model their security level to that of the brick-and-mortar institutions. With respect to security, financial institutions have earned their position as the standards of excellence with their vast experiences and positive reputations. To model after these institutions, Mint implemented triple-layered bank-level security features, including "128-bit SSL encryption and physical security standards."[119] By mimicking banks' security measures, account aggregators could more easily gain consumers' confidence.

Coupled with bank-level security, account aggregators store customers' credentials separately to protect users' identities. For both Personal Capital and Mint, users' bank account credentials are stored separately from their financial data. Personal Capital stores users' credentials on Yodlee's database and never sends credentials to users' web browsers.[120] On the other hand, Mint stores users' credentials on its own server, which is locked in the cage of an unmarked building.[121] This segregation of data storage minimizes risks in the event of a

119 Jennifer Saranow Schultz, "Should You Trust Mint.com?," *Bucks Blog*, 1278443106, http://bucks.blogs.nytimes.com/2010/07/06/should-you-trust-mint-com/.

120 Personal Capital, "Financial Planning Software & Finance Apps," Personal Capital, accessed April 16, 2016, https://www.personalcapital.com.

121 Jennifer Saranow Schultz, "Should You Trust Mint.com?" *New York Times*, accessed February 7, 2016, http://bucks.blogs.nytimes.com/2010/07/06/should-you-trust-mint-com/?_r=0.

security breach. It prevents hackers from obtaining users' bank account logons even if they broke into users' aggregator accounts.

Furthermore, financial account aggregators protect consumers against the predominant vulnerability of screen scraping with innovative security process. The primary concern for screen scraping is its requirement for users to surrender their bank account credentials. However, a developer of Mint addressed this concern by inventing and patenting a system that allows for it to securely access consumers' bank accounts.[122] By targeting this vulnerability, Mint is able to gather and analyze users' bank account information without the risk of compromising users' credentials in the process.

Equally important is the establishment of strict control over internal accesses. Personal Capital maintains that no one can access customers' credentials.[123] On the other hand, Mint's encrypted credentials are only accessible via a key that is split into five pieces, each held by a senior manager.[124] As a result, account aggregators diminish the risk of breaches due to employees' insecure practices. These unique safeguards reduce human errors in causing information security incidents.

In addition to internal security measures, independent third-party reviews bolster account aggregators' system security. Personal Capital operates under Securities and Exchange Commission (SEC) guidelines, which require regular audits by independent auditors.[125] The auditors are to be completely independent for the duration of the audit and any association or relationship with

---

[122] David Michaels, United States Patent: 8566952 - System and method for encrypting data and providing controlled access to encrypted data with limited additional access, 8566952, issued October 22, 2013, http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PALL&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.htm&r=1&f=G&l=50&s1=8,566,952.PN.&OS=PN/8,566,952&RS=PN/8,566,952.

[123] Personal Capital, "Financial Planning Software & Finance Apps."

[124] Jennifer Saranow Schultz, "Should You Trust Mint.com?," *New York Times*.

[125] Personal Capital, "Financial Planning Software & Finance Apps."

the client companies must be disclosed.[126] This condition ensures the reliability and trustworthiness of their evaluations. Lastly, even though Mint does not require audits by securities regulators, it still obtains verification by third parties, TRUSTe and VeriSign.[127] TRUSTe ensures data privacy[128] while VeriSign secures domain infrastructure.[129]

Ultimately, the best safeguard is that most personal account aggregators are not capable of transferring money. Both Mint[130] and Personal Capital[131] are granted read-only access to users' account information. Therefore, there is no risk of money being transferred in and out of users' accounts by malicious actors. This safety net allows users to provide their logon information with less hesitation.

2. Data Sharing

In terms of data sharing, Mint ensures the de-identification of users' personal financial data. To start, Mint collects very minimal PII.[132] The less PII collected, the lower the risk of users' identities being compromised. Furthermore, only users' emails are linked to their accounts.[133] Users' logon information and credentials are never linked to their financial data.[134] Therefore, hackers would not be able to use the financial data from account aggregation services to identify users.

---

126 Office of the Chief Accountant, "Audit Committees and Auditor Independence" (U.S. Securities and Exchange Commission, April 27, 2007), https://www.sec.gov/info/accountants/audit042707.pdf.

127 Mint, "All in One."

128 TRUSTe, "TRUSTe History - Nearly Two Decades of Privacy Innovation," *TRUSTe*, accessed May 14, 2016, https://www.truste.com/about-truste/company-history/.

129 Verisign Inc., "Verisign, Inc. Is A Leader In Domain Names And internet Security - Verisign," accessed May 14, 2016, https://www.verisign.com/.

130 Mint, "4 Things You Didn't Know a Budget App Could Do," October 7, 2013, https://www.mint.com/budgeting-apps/4-things-you-did-not-know-a-budget-app-could-do.

131 Personal Capital, "Financial Planning Software & Finance Apps."

132 Mint, "All in One."

133 Jennifer Saranow Schultz, "Should You Trust Mint.com?," *New York Times*.

134 Ibid.

Correspondingly, aggregation also helps to protect individuals' identities. Even though Mint could share users' data with third parties, it ensures that this data is aggregated or anonymized.[135] Aggregation removes the information necessary for malicious actors to identify individuals. The appropriate level of aggregation safeguards individuals' privacies without compromising quality insights.

[135] Mint, "Mint Bills Privacy and Security," May 7, 2015, https://www.mint.com/mintbills/mobile/privacy_and_security.

III. HEALTHCARE

Conventionally, healthcare data was restricted to those generated sporadically by doctors during office visits. According to the Health Insurance Portability and Accountability Act (HIPAA), protected health information (PHI) includes "individually identifiable health information" from covered entities.[136] PHI comprises of patients' health conditions, prescribed healthcare provisions, and payments for services.[137] In other words, conventional healthcare data refers to patients' records created during doctor's appointments. However, doctor's visits for Americans have dropped to about four times a year on average in 2010[138] with median visit lengths of about 15.7 minutes for primary care.[139] The infrequent and brief visits lead to sparsely documented patient records. These challenges negatively impact the quality of physician care. Therefore, it has become even more difficult for physicians to obtain a holistic view of their patients' health.

In addition, patients do not have ownership to all of their healthcare information. While individuals have the rights to access, amend, or obtain a copy of their medical records under the HIPAA's rules, healthcare providers are still the owners of such data since it is part of their business records.[140] Furthermore, originators that create anonymized or aggregated healthcare data also own them, and these data are not subjected to HIPAA's privacy

136 Office for Civil Rights, "Summary of the HIPAA Privacy Rule," Text, HHS.gov, (May 7, 2008), http://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

137 Ibid.

138 U.S. Census Bureau Public Information Office, "Americans Are Visiting the Doctor Less Frequently, Census Bureau Reports - Health Care & Insurance - Newsroom - U.S. Census Bureau," accessed May 1, 2016, https://www.census.gov/newsroom/releases/archives/health_care_insurance/cb12-185.html.

139 Ming Tai-Seale, Thomas G McGuire, and Weimin Zhang, "Time Allocation in Primary Care Office Visits," *Health Services Research* 42, no. 5 (October 2007): 1871–94, doi:10.1111/j.1475-6773.2006.00689.x.

140 Health Information & the Law, "Fast Facts" (healthinfolaw.org, August 2015).

provisions.[141] In other words, if a person or an organization aggregated a subset of patients' records, this person or organization becomes the owner of such data rather than the patients. Aside from medical records, other types of healthcare information also typically belong to the individual or organization that created it.[142] Thus, patients have very limited ownership and control over their health data.

Despite conventional definitions of data and ownership, the availability of wearable technologies challenges these established traditions. By 2017, eighty million wearable sensors are estimated to be available for health-related usages.[143] The pervasiveness and affordability of low-cost wearable sensors encourage individuals to self-monitor. Additionally, these sensors equip anyone with the capability to continuously track personal biometrics. Wearable technologies allow any individual to generate what traditionally would be considered PHI.

As wearables become omnipresent, individuals will be the biggest and most valuable producers of healthcare data. As of 2012, consumers had generated 68% of the world's 2.8 zettabytes data, which is expected to reach 40 zettabytes by 2020.[144] This is equivalent to about 5,200 gigabyte of data per person, with most of these data captured passively.[145] The volume of consumer-generated data greatly surpasses those from sporadic doctor's visits. Also, this data is much more consistent and comprehensive. With wearable devices, consumers can capture detailed health information at a much higher frequency, without having to make appointments and trips to doctor's offices.

---

[141] Office for Civil Rights, "Summary of the HIPAA Privacy Rule."

[142] Ibid.

[143] Swan, "Sensor Mania! The internet of Things, Wearable Computing, Objective Metrics, and the Quantified Self 2.0."

[144] Christoph Buck Tim Kessler, "Mobile Consumer Apps: Big Data Brother Is Watching You," *Marketing Review St. Gallen* 31, no. 1 (2014): 26–35, doi:10.1365/s11621-014-0318-2.

[145] Lucas Mearian, "By 2020, There Will Be 5,200 GB of Data for Every Person on Earth," *Computerworld*, December 11, 2012, http://www.computerworld.com/article/2493701/data-center/by-2020--there-will-be-5-200-gb-of-data-for-every-person-on-earth.html.

Aside from being the biggest producers, consumers also become the main benefactors of self-tracked data. Individuals can receive personalized feedbacks by quantifying their daily experiences. A Bloomberg article documented individuals that are able to transform their lives with self-experiments, from tracking mood swings to physical changes in the body.[146] For example, an app called Happiness was designed to become a substitute for chemical anti-depressants.[147] By tracking mood changes throughout their day via this app, users are made aware of events that negatively impact their happiness, and they can subsequently make any changes as deemed necessary.[148] Ultimately, consumers are empowered to take on a more active role in managing their health.

In addition to informal uses, the quantified-self data could objectively serve as a second medical opinion. Based on data from the Center for Disease Control and Prevention in 2013, British Medical Journal (BMJ) reported medical error as the third most common cause of death.[149] Though some level of human errors might be inevitable, the medical community could drastically lower the probability by supplementing doctors' subjective medical diagnoses with impartial data. The XPrize's Qualcomm Tricorder competition could achieve this goal in the near future. The competition aims to "stimulate innovation and integration of precision diagnostic technologies, helping consumers make their own reliable health diagnoses anywhere, anytime."[150] Its contestants are to develop a device that could accurately diagnose thirteen health conditions and measure five vital

146 Belinda Lanks, "The Quantified Self: How Cold, Hard Data Improve Lives," *Bloomberg.com*, accessed May 1, 2016, http://www.bloomberg.com/news/features/2015-03-27/the-quantified-self-how-cold-hard-data-improve-lives.

147 Ibid.

148 Ibid.

149 Martin A. Makary and Michael Daniel, "Medical Error—the Third Leading Cause of Death in the US," *BMJ* 353 (May 3, 2016): i2139, doi:10.1136/bmj.i2139.

150 Qualcomm Tricorder XPrize, "Overview," *Qualcomm Tricorder XPRIZE*, September 11, 2015, http://tricorder.xprize.org/about/overview.

signs.[151] The healthcare community could greatly diminish risks for misdiagnosis or mistreatment by using the quantified-self data to either pre-diagnose or verify physicians' evaluations.

Apart from encouraging self-tracking and objective diagnoses, the quantified-self movement delivers a new way for consumers to connect with key stakeholders pertinent to their health. Apple has expanded its role in revamping mobile health by connecting consumers to researchers and healthcare providers. According to Apple, ResearchKit[152] and CareKit[153] can help to advance different dimensions of mobile health with existing technologies embedded in its mobile devices. Apple promotes ResearchKit as a way for researchers to conduct inexpensive and high quality clinical studies without geographical restrictions.[154] Equally important, CareKit allows users to track their recovery and share updates with their healthcare providers.[155]

Correspondingly, Google had unveiled the Baseline Study that parallels in ambition to Apple. According to Wall Street Journal Europe, leaders of the Baseline Study intend to find biomarkers for early disease detection to shift medicine towards preventative care.[156] With participants' data, researchers will use Google's immense computing power to search for patterns that constitute a healthy human.[157] After defining patterns of a healthy human, they could detect

---

151 Ibid.

152 Apple, "Apple - Press Info - Apple Announces Advancements to ResearchKit," accessed April 17, 2016, http://www.apple.com/pr/library/2016/03/21Apple-Announces-Advancements-to-ResearchKit.html.

153 Apple, "Apple - Press Info - Apple Advances Health Apps with CareKit," accessed April 17, 2016, http://www.apple.com/pr/library/2016/03/21Apple-Advances-Health-Apps-with-CareKit.html.

154 Apple, "Apple - Press Info - Apple Announces Advancements to ResearchKit."

155 Apple, "Apple - Press Info - Apple Advances Health Apps with CareKit."

156 Alistair Barr, "Google's New Moonshot Project: The Human Body," *Wall Street Journal*, July 27, 2014, sec. Tech, http://www.wsj.com/articles/google-to-collect-data-to-define-healthy-human-1406246214.

157 Ibid.

deviations that might indicate onsets of diseases. Hence, this project further signifies the immense potential of aggregating and sharing of health data.

Given its overwhelming benefits, the quantified-self movement should continue to expand successfully. To understand its consumer impacts, the following sections examine how the same three factors are operating in the healthcare industry. Current healthcare sector's practices with respect to legislation, technology, and security are discussed in order to understand its implications.

A. LEGISLATIONS AND REGULATIONS

New digital data has led to unexpected sources and uses that might not fall under existing laws. Current legislations and regulations were drafted prior to the availability of digital healthcare data. Therefore, the quantified-self data might not be protected under existing laws. However, to ensure the security and privacy of consumer-generated data, it will be necessary for legislations and regulations to keep pace.

A legislative gap exists in the Health Insurance Portability and Accountability Act (HIPAA) for self-generated data. In 1996, HIPAA established requirements to safeguard data privacy and security for the healthcare industry.[158] Specifically, HIPAA requires covered entities to "implement data protection policies and reasonable security procedures."[159] Covered entities include healthcare providers, insurers, select intermediaries, and business associates that manage PHI for these entities.[160] In this sense, apps or data used within those settings would fall under HIPAA's provisions.[161] When the law was drafted, HIPAA had included all foreseeable entities that could produce and

[158] U.S. Department of Health and Human Services, Office for Civil Rights, "HIPAA Administrative Simplification," March 26, 2013, http://www.hhs.gov/sites/default/files/hipaa-simplification-201303.pdf.

[159] Ibid.

[160] Ibid.

[161] Ibid.

use PHI. Yet, with the quantified-self movement, consumers are rapidly taking on roles similar to that of covered entities, since they not only generate but also use health-related data. However, HIPAA does not apply to data or apps produced solely for personal use. Self-generated data only become PHI once it is shared with covered entities that are designated by HIPAA.

Despite the legislative gap, Federal Trade Commission (FTC) issued guidance to hold developers responsible for being transparent with their intended use of consumers' data. Section Five of the Federal Trade Commission Act prohibits deceptive acts or practices.[162] Under the act, FTC has the authority to prevent app developers from misrepresenting their intended use of consumers' information.[163] With the growth of mobile health apps, FTC took the initiative to help developers with navigating the regulatory requirements by releasing an interactive tool[164] and best practices[165] in April 2016. The web-based tool engages developers by noting relevant laws or regulations, even those beyond FTC's oversight, that need to be considered for their products.[166] Accompanying the tool, FTC also published best security and privacy practices that developers are encouraged to implement.[167]

Aside from the HIPAA and FTC's guidance, developers are also held responsible for the security of medical apps per Food and Drug Administration (FDA) regulations. As a proponent of mobile app development, FDA does not want to restrict the advancement of health applications. Therefore, according to

---

[162] Federal Reserve, "Federal Trade Commission Act Section 5: Unfair or Deceptive Acts or Practices" (Consumer Compliance Handbook, June 2008), https://www.federalreserve.gov/boarddocs/supmanual/cch/ftca.pdf.

[163] Ibid.

[164] Federal Trade Commission, "FTC Releases New Guidance For Developers of Mobile Health Apps," accessed April 20, 2016, https://www.ftc.gov/news-events/press-releases/2016/04/ftc-releases-new-guidance-developers-mobile-health-apps.

[165] Federal Trade Commission, "Mobile Health App Developers: FTC Best Practices," accessed April 20, 2016, https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-app-developers-ftc-best-practices.

[166] Federal Trade Commission, "FTC Releases New Guidance For Developers of Mobile Health Apps."

[167] Federal Trade Commission, "Mobile Health App Developers: FTC Best Practices."

the guidance released in 2015, FDA chose to only regulate a subcategory of healthcare apps that it classifies as mobile medical apps.[168] Mobile medical apps are defined as those that are intended "to be used as an accessory to a regulated medical device" or "to transform a mobile platform into a regulated medical device."[169] FDA believes these devices to be the most risky if they were to fail or not perform as intended.[170] Thus, FDA's efforts are focused mainly on this subset of mobile apps.

Overall, even though HIPAA's coverage is insufficient, FTC and FDA are attempting to keep pace as digital healthcare data becomes more widely available. FTC protects consumer-generated data from deceptive uses by developers, while FDA issued guidance to reduce risks for qualified medical applications. However, HIPAA's provisions are not extended to self-generated information unless it is shared with the designated covered entities. As more digital data are generated, policymakers need to be aware of new sources and uses of PHI that might require additional consideration to ensure the safety and privacy consumers' information.

B. TECHNOLOGY

Most quantified-self applications are integrated via the application program interface (API). APIs govern how one application interacts with another.[171] It exposes a portion of the codes to allow apps to communicate without needing to reveal all of its proprietary programs. With APIs, applications can transmit information to one another. For instance, APIs could share users' credentials between different apps, so users can conveniently sign into multiple applications

168 U.S. Department of Health and Human Services et al., "Guidance for Industry and Food and Drug Administration Staff" (Food and Drug Administration, February 9, 2015), http://www.fda.gov/downloads/MedicalDevices/.../UCM263366.pdf.

169 Ibid.

170 Ibid.

171 Brian Proffitt, "What APIs Are And Why They're Important," ReadWrite, September 19, 2013, http://readwrite.com/2013/09/19/api-defined/.

with a single authentication. The following sections examine current best practices of healthcare aggregators.

1. Data Aggregation

Users obtain a holistic and customizable view of their health and fitness statuses with real-time dashboards. Apple's Health application and HealthKit, open API framework, consolidate multiple data sources to generate a simple summary dashboard.[172] The different data sources include information collected via device sensors, third-party apps, and users' manual inputs.[173] Users have the option to select the activities they want to be displayed. Each activity is graphed separately as a bar chart (Figure 6). By scrolling through, users can see their activity levels for different time intervals: day, week, month, or year.

Figure 6. Dashboard of Apple's Health.[174]

172 Apple, "iOS 9 - Health," Apple, accessed April 18, 2016, http://www.apple.com/ios/health/.

173 Ibid.

174 Source: Apple, "Use the Health App on Your iPhone or iPod Touch," Apple Support, accessed June 12, 2016, https://support.apple.com/en-us/HT203037.

Released by Harvard Medical students, Sherbit is another app that allows users to merge an even greater variety of data sources. Sherbit aims to provide context to users' online information by helping consumers access data from social media apps, even if those apps are not directly related to health and fitness.[175] For example, if an individual were interested in how "likes" on their tweets impacts their activity level, the user would grant Sherbit permission to retrieve data from Twitter and Fitbit.[176] Then, the app would display a graph of the number of likes over time (Figure 7). Another graph for the number of steps recoded by Fitbit would be displayed in a similar manner. Even though data from each source is graphed separately, these two charts are stacked to provide a visual comparison.

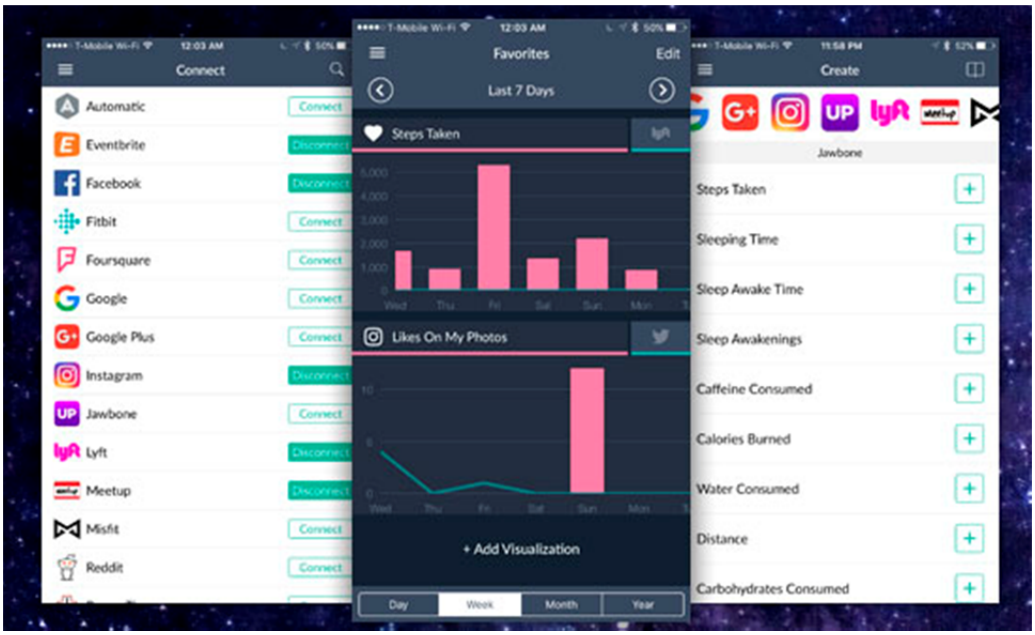

Figure 7. Dashboard of Sherbit.[177]

[175] Adam Dachis, "Sherbit Visualizes and Interprets All the Data Your Online Services Collect," *Lifehacker*, accessed June 12, 2016, http://lifehacker.com/sherbit-visualizes-and-interprets-all-the-data-your-onl-1779567985.

[176] Ibid.

[177] Source: Ibid.

Aside from displaying summarized information, health apps attempt to proactively monitor users' health via reminders and alerts. Google Fit, an android application, allows users to set personal fitness goals.[178] Its daily activity and step goals can be modified based on personal preferences.[179] Furthermore, Google Fit also sends periodic notifications of goal updates and reminders to encourage users to continue towards their fitness goals.[180] Apart from fitness, Apple's CareKit tracks recovery plans after surgeries or treatment plans based on medical diagnoses.[181] It provides insights by comparing designated treatment plans to patients' recovery progresses.[182] The Insight module from CareKit displays tips and alerts to ensure that users stay on track through recovery (Figure 8).

[178] Dan Graziano, "The Complete Guide to Google Fit," *CNET*, accessed April 18, 2016, http://www.cnet.com/how-to/the-complete-guide-to-google-fit/.

[179] Ibid.

[180] Ibid.

[181] Caitlin McGarry, "Apple's CareKit Gives You and Your Doctors a Better Understanding of Your Health," *Macworld*, March 21, 2016, http://www.macworld.com/article/3046513/software/apples-carekit-gives-you-and-your-doctors-a-better-understanding-of-your-health.html.

[182] Ibid.

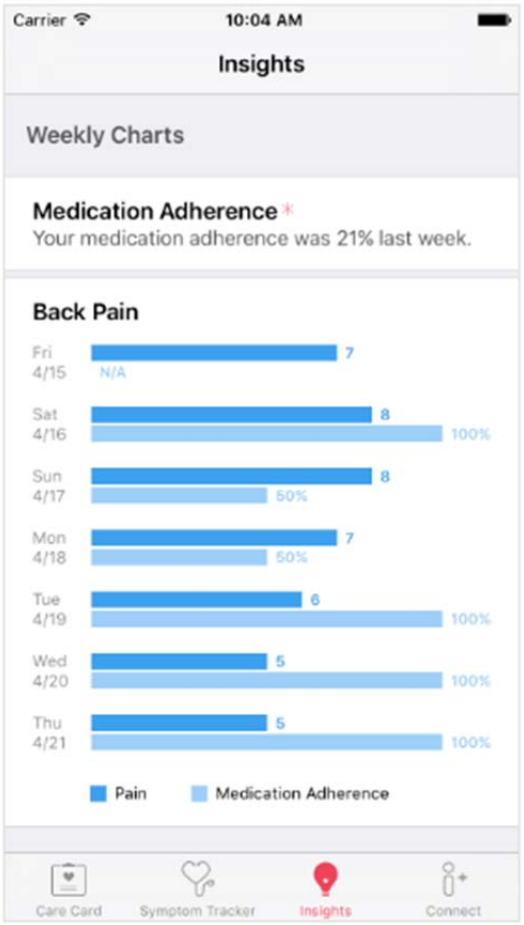

Figure 8. Dashboard of CareKit's Insight Module.[183]

2. Data Sharing

Though not explicitly useful, consumers do have the option to export their data from Apple's Health app. The Health app allows users to export their data in an Extensible Markup Language (XML) format.[184] The export option automatically creates a zip file for users to email it to themselves or others.[185] The file contains all of an individual's health data that has been captured via the

[183] Source: CareKit, "Overview Document," accessed June 13, 2016, http://carekit.org/docs/docs/Overview/Overview.html.

[184] Jonny Evans, "How to Export Apple Health Data as a Document to Share," accessed June 12, 2016, http://www.computerworld.com/article/2889310/how-to-export-apple-health-data-as-a-document-to-share.html.

[185] Ibid.

app. Yet, the XML file consists of codes that seem incomprehensible to the average consumer (Figure 9).

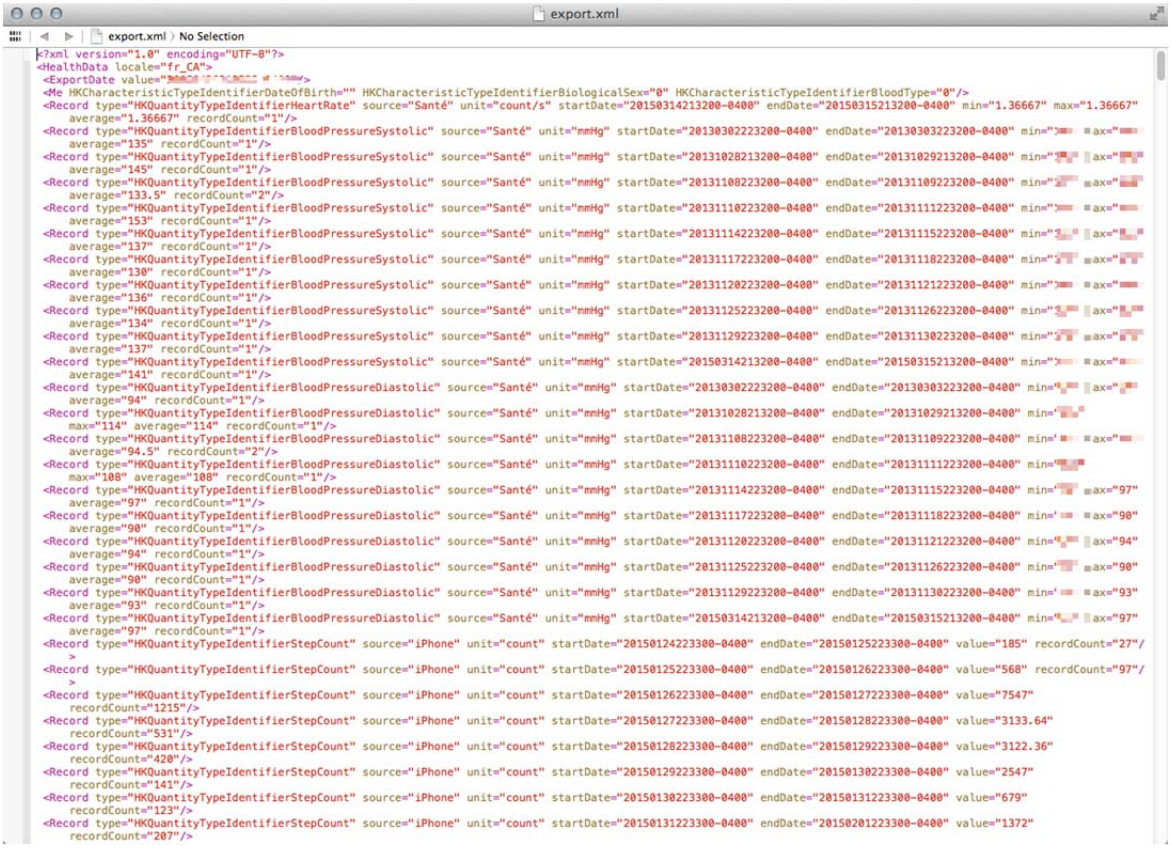

Figure 9. XML Data Export File from Apple's Health.[186]

Aside from accessing raw data, users have the option to share their recovery progresses. Consumers can keep their family, friends, and health professionals updated on changes in their heath statuses with the Connect module from Apple's CareKit.[187] Sharable information includes treatment plans from the Care Card, improvements tracked via the Symptom and Treatment

[186] Source: Stack Exchange Inc., "Icloud - View iOS Health Data Externally - Ask Different," accessed July 12, 2016, http://apple.stackexchange.com/questions/167671/view-ios-health-data-externally.

[187] Apple, "Apple - Press Info - Apple Advances Health Apps with CareKit."

Tracker, and effectiveness of the treatment plan via the Insight Dashboard.[188] The Connect module facilitates two-way communications necessary to ensure efficient and effective care.

Finally, healthcare apps can also connect users to medical researchers. Researchers can use the ResearchKit to design experiments with participants' mobile health data.[189] A news review of ResearchKit states that it "accesses sensors in the iPhone, including the accelerometer, microphone, gyroscope, and GPS sensors, in order to gain insight into [users'] gait, motor impairment, fitness, speech, memory, and more."[190] Once participants agree to share their health data via the app, researchers use the credentials they receive to retrieve information from participants' phone.[191] The open-source software kit empowers universities and research teams to reach participants for medical trials and studies without geographical restrictions.

C. SECURITY

While APIs provide the necessary data interoperability for healthcare applications, they also carry associated vulnerabilities. A leading technology research and advisory firm, Ovum Consulting, recently published survey results indicating a lack of clarity on APIs' security responsibilities.[192] These responsibilities seem to be almost evenly split between the security and developer teams.[193] Due to vague accountability, it is imperative to prioritize

188 Ibid.

189 Caitlin McGarry, "ResearchKit at 6 Months: 100,000 People Now Using Medical Apps," October 15, 2015, http://www.macworld.com/article/2993838/ios/researchkit-at-6-months-100-000-people-now-using-medical-apps.html.

190 Elyse Betters and Mike Lowe, "Apple ResearchKit and CareKit: Everything You Need to Know - Pocket-Lint," March 21, 2016, http://www.pocket-lint.com/news/133132-apple-researchkit-and-carekit-everything-you-need-to-know.

191 Ibid.

192 Marketwired, "New Ovum Study Looks at API Security Practices, Revealing Basic Security Measures and Attack Vectors Overlooked and Disconnect Between Developers and IT Security Teams," *Yahoo Finance*, accessed June 12, 2016, http://finance.yahoo.com/news/ovum-study-looks-api-security-130000389.html.

193 Ibid.

security with the growth of health applications and APIs. The next sections discuss best security practices in data aggregation and sharing.

1. Data Aggregation

Quantified-self aggregators secure users' data by storing it locally. Sherbit stores all users' information locally.[194] By confining users' data to their devices, Sherbit limit the potential impact of a breach. However, Sherbit is planning on giving users the option to store and sync their health data to a central server in the future.[195] Still, users could opt-out if they prefer to keep their data locally.[196]

Another component to information security is data transmission. Google Fit ensures security in its data collection with authenticated and encrypted connections.[197] Unless both of these requirements are met, it is impossible for users' devices to communicate with Google's server.[198] This security measure prevents information from being intercepted without users' consent or awareness.

Aside from data security, healthcare companies focus on preventing security incidents due to employees' oversight. Sherbit promises necessary trainings and security procedures to ensure the safety of users' information.[199] Even though its employees can access users' information, Sherbit is confident in its trainings for employees to appropriately handle sensitive healthcare

194 Sherbit, "About," Sherbit- Personal Analytics, accessed May 15, 2016, https://www.sherbit.io/about/.

195 Ibid.

196 Ibid.

197 Joram Teusink, "Android Wear and Google Fit and Its Privacy and Security ~ Teusink," accessed January 25, 2016, http://www.teusink.eu/2015/02/android-wear-and-google-fit-security-privacy.html.

198 Ibid.

199 Sherbit, "Sherbit Privacy Policy," Sherbit- Personal Analytics, accessed May 14, 2016, https://www.sherbit.io/privacypolicy/.

information.[200] Promoting security awareness, Sherbit's targeted trainings aim to lower the risk of data breaches due to employees' mishaps.

Lastly, health data aggregators are mixed in their approaches to ensure HIPAA compliance. Developers wanting to connect to Apple's HealthKit need to make sure that their apps comply with the HIPAA or other regulations as applicable.[201] Apple let external developers take on responsibilities to ensure regulatory compliance, specifically in regards to HIPAA's privacy provisions. On the other hand, Google bluntly states that Google Fit is non-compliant with HIPAA and discourages users from subjecting its application to any HIPAA-related usage.[202] Google warns against uses of Google Fit that might fall under the purview of HIPAA or FDA.[203] This declaration relieves Google of any legislative or regulatory liabilities and places these burdens on its users instead.

2. Data Sharing

Developers of healthcare apps prevent misuses of users' information by setting stringent guidelines. Both Apple's HealthKit[204] and Google Fit[205] prevent sensitive data from being used for advertising or purposes other than intended. Likewise, Sherbit promises not to share any information with third parties without users' consent, except under extreme circumstances. These strict policies are designed to ensure consumer privacy.

---

200 Ibid.

201 Apple, "HealthKit Framework Reference," accessed May 15, 2016, https://developer.apple.com/library/ios/documentation/HealthKit/Reference/HealthKit_Framework/.

202 Google Fit, "Terms and Conditions," Google Developers, accessed May 15, 2016, https://developers.google.com/fit/terms.

203 Ibid.

204 Roberto Baldwin, "Apple Updates HealthKit Privacy Policy to Ban Selling Data," The Next Web, August 28, 2014, http://thenextweb.com/apple/2014/08/28/apple-updates-healthkit-privacy-rules-keep-health-data-hands-advertisers/.

205 David Nield, "Google Fit v Apple Health," Wareable, accessed May 15, 2016, http://www.wareable.com/sport/google-fit-vs-apple-health.

Moreover, consumers are granted control over third-party accesses to further restrict unwanted use of their data. They can set different permission levels for third parties for both Apple's HealthKit and Google Fit.[206] Since both apps are open to developers, users' control over third-party accesses is a necessity.[207] Furthermore, based on developers' best practices for ResearchKit, users should have control over data shared with researchers and data shared by researchers with others.[208] Participants should also be given the option to leave the research at any point.[209] These emphases on users' control over third-party accesses further reinforce users' ownership and prevent deceptive misuses.

206 Max, "Best Digital Health System: Google Fit vs. Apple HealthKit," Appcessories - App-Enabled Accessories and Wearables, November 27, 2015, http://www.appcessories.co.uk/the-best-digital-health-system-google-fit-vs-apple-healthkit/.

207 Ibid.

208 GitHub, Inc., "ResearchKit/ResearchKit," *GitHub*, accessed May 30, 2016, https://github.com/ResearchKit/ResearchKit.

209 Ibid.

IV. COMPARATIVE ANALYSIS VIA PORTER'S FIVE FORCES FRAMEWORK

Overviews of financial services and healthcare reveal that each industry has its own legislations, technological developments, and security processes. These characteristics impact the quality and security of services that consumers receive. Since consumers are policymakers' main concern, it is imperative to understand how financial services industry's practices benefit its consumers. The comparison would also reveal healthcare industry's areas needing improvement.

For the comparative analysis, Porter's Five Forces Framework is applied to explore how the two industries' relate to their respective consumers. Traditionally, prospective firms use Porter's Five Forces Framework to assess competitive forces in developing strategies for entering an industry.[210] However, this thesis is using the framework to demonstrate how the competitive dynamics of each industry benefits its respective users. The comparison is organized based on the five forces, which include competitive rivalry, threat of new entrant, threat of substitute products or services, bargaining power of suppliers, and bargaining power of buyers (Figure 10).[211]

[210] Michael E. Porter, *Competitive Strategy: Techniques for Analyzing Industries and Competitors: With a New Introduction*.

[211] Michael E. Porter, "The Five Competitive Forces That Shape Strategy," *Harvard Business Review*, January 2008, 79–93.

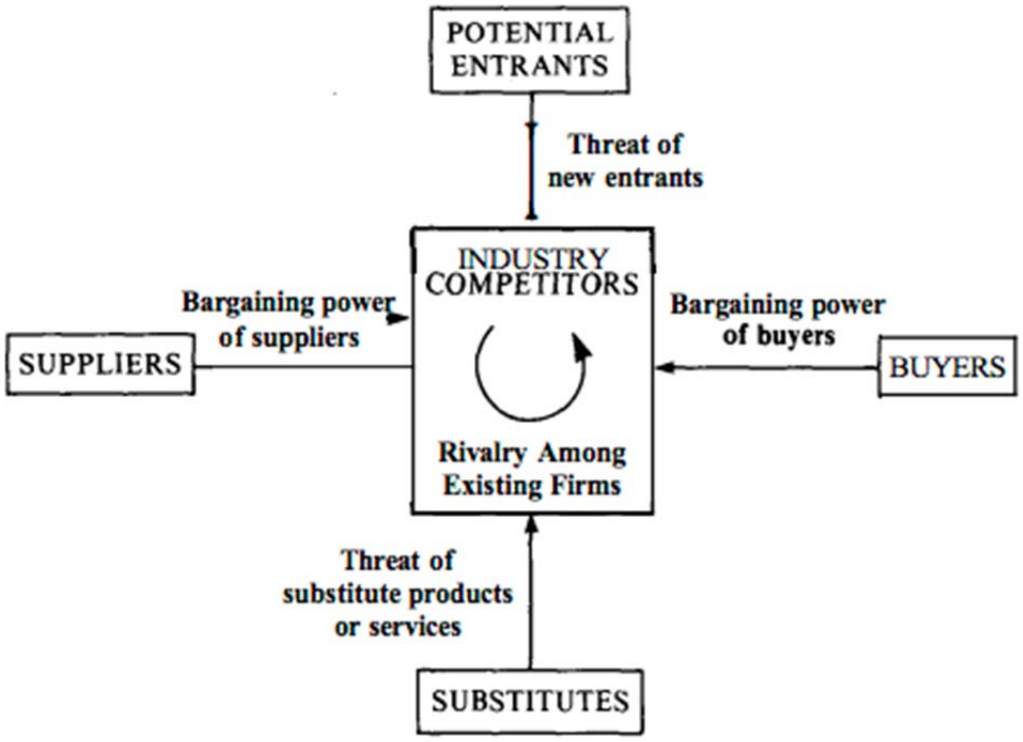

Figure 10. Diagram of Porter's Five Forces Framework.[212]

The five forces can be categorized into two types of competition, vertical and horizontal.[213] Vertical competition describes interactions between firms at successive stages of a supply chain, such that manufactures take on a more important role.[214] Of the five forces, bargaining power of suppliers and buyers are considered to be part of the vertical competition. In contrast, horizontal competition refers to interactions between firms at the same stage of a supply chain.[215] In this case, firms' decisions on pricing, investment, or research would

[212] Source: Michael E. Porter, *Competitive Strategy: Techniques for Analyzing Industries and Competitors: With a New Introduction*.

[213] Team FME, *Porter's Five Forces* (www.free-management-ebooks.com, 2013), http://www.free-management-ebooks.com/dldebk-pdf/fme-five-forces-framework.pdf.

[214] Jie Wei and Jing Zhao, "Pricing Decisions for Substitutable Products with Horizontal and Vertical Competition in Fuzzy Environments," *Annals of Operations Research*, February 4, 2014, 1–24, doi:10.1007/s10479-014-1541-6.

[215] Ibid.

have more of an impact on an industry's competitive dynamics.[216] The remaining three forces are considered to be part of horizontal competition: competitive rivalry, threat of new entrants, and threat of substitute products or services.

One of the key horizontal forces is competitive rivalry. Competitive rivalry describes the "intensity of rivalry among firms."[217] Rivalry exists because firms are mutually dependent and incumbent firms seek opportunities to gain profit.[218] There are a number of factors impacting the intensity of rivalry, including number of firms, market growth, product differentiation, exit barriers, and rival diversity.[219]

Another one of the three horizontal forces is threat of new entrants. The threat of new entrants describes how potential new competitors threaten existing competitors.[220] Increasing barriers for firms to enter an industry lowers this threat. Factors influencing barriers to entry include government policies, patents and proprietary knowledge, and economies of scale.[221]

Thirdly, threat of substitutes is the last of the horizontal forces. Substitute products or services refer to those from a different industry that can be used in place of the product or service of interest. The threat of substitutes refers to the potential negative impact of a substitute on the product of interest.[222] Typically, this effect is derived from the impact of changes in price of a substitute on the demand for the product in question.[223] However, other factors could also raise concerns, such as technology and changing environments.[224]

---

216 Ibid.

217 Michael E. Porter, *Competitive Strategy: Techniques for Analyzing Industries and Competitors: With a New Introduction*.

218 Ibid.

219 QuickMBA, "Porter's Five Forces," accessed June 25, 2016, http://www.quickmba.com/strategy/porter.shtml.

220 Michael E. Porter, *Competitive Strategy: Techniques for Analyzing Industries and Competitors: With a New Introduction*.

221 QuickMBA, "Porter's Five Forces."

222 Ibid.

223 Ibid.

224 Ibid.

First of the vertical forces is bargaining power of suppliers. Suppliers are those that provide raw materials to the industry of interest.[225] Hence, the bargaining power of suppliers describes suppliers' leverage on an industry's competitive dynamics. Key factors impacting bargaining power of suppliers include supplier concentration, cost to switch suppliers, and credible threat of forward integration.[226]

Last of the five forces, bargaining power of buyers is the other vertical force. Power of customers describes how much buyers could influence an industry's dynamics.[227] For instance, in a market with strong buyer power, customers set the price for goods.[228] Factors impacting bargaining power of buyers are buyer concentration, volume of purchase, and credible backward integration threat.[229]

A. COMPETITIVE RIVALRY

Strategic diversity and product differentiation are two indicative factors of competitive rivalry. Strategic diversity refers to an industry consisting of companies with unique approaches to conduct businesses.[230] These companies tend to position themselves differently from others. The unpredictability of their unique strategies increases rivalry intensity.[231] Conversely, product differentiation describes the bases for distinguishing a firm's product versus that of its competitors'.[232] Higher product differentiation lowers competitive rivalry. Based on conventional definitions, these two factors have opposite effects on

225 Michael E. Porter, *Competitive Strategy: Techniques for Analyzing Industries and Competitors: With a New Introduction*.

226 QuickMBA, "Porter's Five Forces."

227 Michael E. Porter, *Competitive Strategy: Techniques for Analyzing Industries and Competitors: With a New Introduction*.

228 QuickMBA, "Porter's Five Forces."

229 Ibid.

230 Ibid.

231 Ibid.

232 Ibid.

firms' rivalry intensity. However, from the policymakers' perspective, both stimulate innovations that benefit consumers in different ways.

By examining the two industries, it is clear that products from both sectors offer basic analogous capabilities. For instance, most services include a centralized dashboard for clear and holistic visualization. The dashboards allow users to have instant access to multiple sources of data. Moreover, these aggregators include rudimentary abilities for proactive goal monitoring, which is imperative to promote behavioral changes. Additionally, the alert features guide users to progress toward personal goals.

In contrast to healthcare services, financial account aggregators provide more comprehensive feedbacks for their users. Even though both industries employ some form of proactive monitoring, the two sectors design this feature to serve different purposes. Health apps are focused on informing users of their progress and reminding them of their goals. However, financial aggregators do not strictly inform and remind users, but instead look to alert unwary users of suspicious activities as well as noting personalized advices and recommendations.

Furthermore, personal financial aggregators' sophisticated algorithms enable automation and complex analysis. Focused on reaching users' financial goals, account aggregators are capable of automatically adjusting wealth allocations to optimize returns. With such automation, account aggregators could instantly adapt to market fluctuations. By the same token, personal financial services also provide the capability to perform predictive analysis. For example, users could estimate the impact of various life events on their financial goals. This feature not only allows users to plan for such milestones, but also prepares them financially and mentally.

Based on these observations, healthcare aggregators are much more strategically diverse. The first example of healthcare aggregators' strategic diversity is their attempt to target both segments: users and developers. By

launching applications and APIs, healthcare leaders aim to accommodate both types of customers. Additionally, healthcare services are designed for a variety of purposes. For instance, Google Fit is solely intended for tracking personal fitness data, while Apple's apps and APIs are healthcare-centric. Sherbit offers to serve an even broader objective, capable of connecting most of users' data sources. All three healthcare competitors are strategically distinguishing themselves by appealing not only to different customer segments but to different consumer needs as well.

On the contrary, financial account aggregators are more strategically similar. Most aggregators aim to offer users a one-stop shop for all services. Account aggregators tend to serve a single purpose, centered on holistic financial management despite some level of specialization. For example, Mint is mainly for budget management versus Personal Capital for investments, but each still have the capability to manage other financial aspects. Personal financial services accommodate a wider range of users with these well-rounded tools. Each aggregator, despite their specializations, can meet all of the users' basic financial needs.

Along with similar strategies, personal financial aggregators have a higher level of product differentiation. Account aggregators include unique features to increase product distinction. In particular, Mint offers free credit score checks as well as noting impacts on users' credit scores based on their specific financial habits. Additional notable elements are Betterment's automated tools and Personal Capital's life event impact analysis. Firms distinguish their products by developing unique features that generate value for the consumers. As a result, consumers benefit from these analytical innovations.

In contrast, healthcare aggregators demonstrate much lower product differentiation. Healthcare apps deliver basic aggregation services with simple visualizations. Typical user interfaces for healthcare apps generally consist of bar charts that indicate individuals' activity levels. While CareKit attempts to provide slightly more analysis with its alerts, most apps fail to go beyond simple analytics.

Consumers are benefiting from each industry's competitive rivalry in different ways. From the personal financial industry, consumers receive products that offer comprehensive essential services supplemented with novel analyses. In contrast, though the healthcare industry delivers products with similar functionalities, these products are designed to target diverse customer segments and consumer needs. Under both circumstances, consumers are benefiting from innovative products, even if the focuses of innovation differ.

B. THREAT OF NEW ENTRANTS

The threat of new entrants is inversely dependent on barriers to entry. Two key barriers to entry for the healthcare and personal financial sectors are government policies and patented information. In the following sections, consumer benefits based these two factors are evaluated for each sector.

1. Comprehensive Legislations as Barriers to Entry

Laws and regulations represent one form of barrier to entry. These standards obligate time, effort, or money to ensure compliance. Consequently, stringent legislations are more costly to comply with, resulting in a higher barrier to entry. From the consumers' perspective, some level of barrier in this aspect is necessary since adequate legislation ensures the security and privacy of their information.

Both industries have some laws in place to ensure data privacy and security. The legislative safeguards protect users who adopt aggregation services. These protections aim to hold developers responsible for data security, transparent privacy policies, and honest intended use of consumers' data.

However, healthcare legislation still lacks comprehensive coverage. HIPAA does not cover self-generated healthcare information. While FTC supplemented existing regulations with a new tool and best practices for the developers, FDA only issued stricter guidance for services that qualify as medical

apps. These efforts are healthcare regulatory agencies' attempts to patch the gap in HIPAA's coverage.

Furthermore, the lack of accountability allows some healthcare developers to circumvent regulatory requirements. Google publically proclaims Google Fit's noncompliance with HIPAA and discourages any usage that might trigger HIPAA or FDA guidance. This practice forces the consumers to take on the responsibility in differentiating between compliant versus non-compliant usage. Similarly, instead of vetting the associated apps, Apple requires external developers interested in connecting to HealthKit to obtain the necessary compliance for their apps. These companies transfer these liabilities to its users and developers due to a lack of legislative accountability.

In contrast, the personal financial sector adapted existing regulations to accommodate technological advancements. The financial services industry did not announce new regulations when account aggregators had begun to take hold in the market. Even though the Federal Reserve Board has yet to issue clarifications regarding the applicability of Regulation E, legislators interpreted the Gramm-Leach-Bliley Act (GLBA) to include account aggregators. No regulations were added because current ones are sufficient in guiding account aggregator developments and protecting the consumers.

Based on the comparison, the personal financial industry would have a higher barrier to entry. With comprehensive legislative requirements, entrance to financial services industry is more costly to prospective developers. The higher cost of entry deters low quality firms that are unwilling to invest the necessary time and effort. As a result, the personal financial industry would be better positioned to continue to deliver secure services to its consumers.

2. Innovative Security Measures as Barriers to Entry

Due to data sensitivity, superior security measures become another form of barrier to entry. Consumers are more inclined to adopt products with hardened security measures. To earn consumers' confidence, developers must ensure that

their security features provide unparalleled protection. By offering the best-in-class security, developers could more effectively compete with others. Ultimately, this drive to outperform their competitors makes security measures a natural deterrent for those less qualified. Most importantly, it also motivates firms to provide the most secure services for their users.

The basic security framework for information flow exists in both industries. Both sectors take on extra precautions with respect to the security of data storage, internal accesses, and sharing of information with third parties. These measures are imperative to the establishment of a secure environment for consumers to freely share personal data. The minimal requirements for information security have been met by both industries.

Yet, the personal financial industry provides more innovative protection. Mint patented a new process for it to securely access consumers' financial information with their bank credentials. Mint's patent represents proprietary knowledge that cannot be replicated. Therefore, the patent owners gain an exclusive advantage over their competitors.

As a barrier to entry, personal financial industry's pioneering security measures result in secure services for its consumers. In essence, patented security process raises the barrier to entry. This emphasis on security innovation reinforces it as a key deterrent for unqualified competitors and prevents inferior products from being released into the market. Accordingly, users of personal financial aggregators would continue to benefit from the industry's higher security and legislative barriers.

C. THREAT OF SUBSTITUTE PRODUCTS OR SERVICES

Substitutes are products from other industries that perform similarly to the ones of interest. Threat from substitutes drives up competitive forces,[233] which also motivates firms to innovate in order to distance themselves from potential

[233] Ibid.

substitutes. Ultimately, consumers are the ones benefiting from these technological advancements. The following sections examine a sample of potential substitutes: Microsoft Excel, If This Then That (IFTTT), and FreshBooks. Microsoft Excel represents the most widely accessible substitute product, while IFTTT and FreshBooks are examples of different alternatives.

1. Microsoft Excel

Microsoft Excel is one of the most prominent substitutes for data aggregators in both sectors. Providing similar services as the aggregators, Excel has the necessary functions to enable manual data aggregation and sharing. It allows users to create different types of visualizations as well as share raw and aggregated data. While it does require a fee to install, most individuals already own Microsoft Office Suite for other purposes. Also, since it is a popular tool, most should already be familiar with its basic functionalities. These qualities render Excel as one of the most viable substitute.

In terms of security, Excel do not have extensive safeguards built-in, but it is also less vulnerable to unwanted accesses. Excel allows users to encrypt and password-protect their files. These security features are far inferior in complexity and completeness than those available for financial and healthcare aggregators. However, Excel data has a lower risk of being hacked or used by third parties since it is typically stored locally. The decentralized storage restricts external accesses to these data.

Although locally stored data limits security risks, it also greatly diminishes the benefits derived from mass aggregation. Consumers could compare their financial or health statuses to that of their peers' via centralized databases. This shared data also helps to advance research by enabling trend investigations and population baseline studies. These advantages cannot be realized if all data are separately stored on personal laptops.

Self-recorded data allows for more flexible analysis and visualization despite its disadvantages. Users could obtain a holistic view of their financial

statuses via account aggregators. On the contrary, using Excel, they would need to manually retrieve and record information from each account or activity separately. Also, a delay exists for self-recorded data since the information is typically captured after the activity took place. Nonetheless, this delay is compensated by the flexibility Excel provides. With Excel, users are able to create a variety of visualizations and analysis from any portion of recorded data. Though healthcare and financial aggregators provide some level of dashboard customization, neither is capable of allowing users the freedom to visualize or analyze any subset of collected data.

Similar to Excel, personal financial aggregators allow users to access and share usable raw data, whereas the opposite is true for healthcare. Comparable to Excel, personal financial aggregators provide users with raw CSV files. These files, like Excel files, can also be shared with anyone for customizable analysis and visualization. However, users of healthcare aggregators could only export their data as an XML file that is not as useful. Although it can also be shared with anyone, XML files contain codes that are not readily usable for typical consumers wanting to manipulate their raw data.

Furthermore, financial account aggregators are able to provide more sophisticated analyses. These services include automation, predictive analysis, and personalized recommendations. More complex analyses and features typically require linkages to external programs. Since Excel does not connect users' data to any other programs or services, it is limited in its ability to provide more advanced capabilities.

Based on the assessment, threat of substitution from Excel is valid for both industries, but it is lower for personal finance. Excel can meet users' needs for data aggregation and sharing. It also performs comparably. While it makes mass aggregation more difficult, Excel has many qualities that render it to be a viable substitute.

Nevertheless, the threat of substitution is lower for the financial services industry versus healthcare, because personal financial aggregators offer users access to usable raw data similar to that from Excel. Furthermore, it provides users with more advanced analytical tools versus both Excel and healthcare aggregators. Therefore, Excel is less of a threat to personal financial aggregators.

2. Other Sources of Substitutes: IFTTT and FreshBooks

Aside from Excel, aggregation services face threats from products that enable automation of app data. If This Then That (IFTTT) is a web service that automates tasks designated by users with conditional statements.[234] Also known as "recipes," these conditional statements take on the form of "if p, then q," where if p is true, then q is also true.[235] For example, IFTTT users can track their fitness goals by connecting Fitbit to Twitter[236] with "if daily Fitbit steps reaches 10,000 steps, then share this achievement via Twitter." Analogous to Sherbit, IFTTT's users have greater flexibility in connecting a variety apps data.

Additionally, as the experienced industry, financial services have more prevalent substitutes. Electronic financial account aggregation had appeared between 1999 and 2000 in the United States,[237] whereas healthcare data aggregators have only started to emerge in recent years. Given its success, the concept of account aggregation has been reapplied to related industries. In particular, FreshBooks is designed for small business owners to track expenses.[238] Similar to Mint, this service also allows for the automatic import and

---

234 IFTTT, "IFTTT, IFTTT / Connect the Apps You Love," accessed August 8, 2016, https://ifttt.com/.

235 Stanford University, "An Introduction to Philosophy," accessed August 8, 2016, https://web.stanford.edu/~bobonich/dictionary/dictionary.html.

236 IFTTT, "Tweet When You Achieve Your Daily Fitbit Step Goal," IFTTT / Connect the Apps You Love, accessed August 8, 2016, https://ifttt.com/recipes/175106-tweet-when-you-achieve-your-daily-fitbit-step-goal.

237 Fujii et al., "E-Aggregation."

238 FreshBooks, "FreshBooks Cloud Accounting," accessed August 8, 2016, https://www.freshbooks.com/expenses-and-receipts-tracking.

categorization of account information from banks and credit cards.[239] Though intended for small businesses, FreshBooks users could easily adopt it for their personal expenses as well.

In conclusion, both financial services and healthcare sectors have comparable threats from substitutes. Though Excel is less of a threat to financial account aggregators, substitutes are more available given financial account aggregation's maturity. On the other hand, even though they have only been developed recently, healthcare aggregators are already facing threats from services offering more flexibility in data automation, such as IFTTT. Thus, the two industries face equivalent threats from substitutes, resulting in similar influences on consumer experiences.

D. BARGAINING POWER OF SUPPLIERS

Industry suppliers directly impact aggregation technologies. Since personal financial aggregators mostly use the screen scraping method, their key supply is banks' websites. On the other hand, device manufactures are healthcare app and API's key suppliers, because healthcare aggregators gather data via devices' sensors. These suppliers are powerful because their products are important inputs to the respective industries and they present credible threats of forward integration.

For financial services, account aggregators based on screen scraping rely heavily on the consistency of banks' website layouts. Screen scraping is one of the most popular methods of aggregation. This method logs into users' accounts with their credentials and grabs information from users' account webpages. Perpetual changes to these websites are detrimental to aggregators' operations, because the aggregators would need to be updated continuously to ensure that they are capturing accurate bank account information. The mechanics of screen scraping makes it highly dependent on banks' website layouts.

[239] Ibid.

On the other hand, healthcare aggregators are highly dependent on device manufactures. Healthcare applications and APIs typically gather users' data via phones' or other devices' sensors. Information accuracy and security are contingent on the availability and reliability of devices' embedded technologies and security measures. In order to track biometric data precisely and securely, the technical capabilities and security features of devices' sensors are of the utmost importance. Therefore, device manufactures could shape the development of healthcare aggregators.

Suppliers in both industries produce important inputs that impact its buyers' information gathering process and data quality. Financial account aggregators need banks' website layouts to remain relatively stable in order to sustainably generate accurate information. Changes to website layouts not only impact their operations but their product quality as well. For healthcare aggregators, devices serve as both the information gatherers and delivery portals. Therefore, product quality and security is heavily dependent on devices' capability to accurately and securely measure, aggregate, and deliver consumers' data.

While both industries rely heavily on suppliers' inputs, healthcare aggregation services have a higher credible threat of forward integration. The threat of forward integration refers to the possibility of a supplier becoming a competitor. In the financial services sector, banks threaten third-party account aggregators. Banks are capable and encouraged to provide account aggregation services for their customers to prevent them from having to share their account logins with third parties. However, this possibility is low because banks do not typically have the technical skillset required to develop quality services comparable to that from third-party developers. Yet, forward integration is already evident in the healthcare sector. For instance, Apple, as a device manufacturer, has already released some of the most recognizable health aggregation apps and APIs. With successful precedents, this trend is unlikely wean. Thus,

healthcare aggregators have a higher credible threat of forward integration and, therefore, higher bargaining power of suppliers.

For this reason, developers' motivations vary depending on whether they take on the additional role as suppliers. The healthcare sector already has a strong presence of corporate ownership, resulting in data silos. With healthcare suppliers' greater bargaining power, data interoperability would not be a priority for its developers. Since healthcare developers tend to be the same as device manufacturers, they are more likely to focus on their apps or APIs' compatibility with their own devices. Thus, integrating data with other devices or apps is probably less of a concern. Conversely, personal financial aggregators typically originate from third parties. Hence, these third-party developers' key proposition would be to integrate data across various sources, thereby ensuring interoperability as their top priority.

Consequently, users of financial account aggregators receive more interoperable products. Data interoperability is essential for users of aggregation services. By definition, aggregators should be able to integrate data across a variety of sources. As noted previously, personal financial aggregators are better positioned to meet this need, because their third-party developers' have motivations that are better aligned with consumer interests.

E. BARGAINING POWER OF BUYERS

Bargaining power of buyers is comparable for both industries. Given that consumers in the two industries use aggregators in similar manners, buyers are likely to exert equivalent influences. In terms of consumer benefits, higher bargaining powers indicate that users would have a greater leverage in demanding product improvements. Nonetheless, the following analyses reveal that buyers of both industries have moderate bargaining power.

Buyers have low bargaining power because of their large population, need for only one aggregator, and low concentration. Buyers' bargaining powers are diluted, because of the large pool of potential users. Aggregators are designed to

appeal to the general public; therefore, the number of prospective consumers is high. Also, each user typically needs only one data aggregation service, since it would defeat the purpose of centralizing information if multiple aggregators are adopted. This adoption behavior also contributes to a low concentration of buyers, because the ratio of consumer to product is expected to be relatively equal. Under those circumstances, all three factors lower the bargaining power of buyers.

However, these three factors are slightly offset by the low switching cost. As most aggregators are available for free, the main cost to switch is users' effort spent in adopting a new technology. Since the effort exerted in adopting these products cannot be recuperated, it could be viewed as a form of sunk cost, which is a type of cost that cannot be recovered once invested.[240] This analogy indicates that users' efforts spent in learning one product is essentially wasted once they decide to switch to another product. Although, it is important to point out that this cost to switch would be insignificant, since aggregators are designed to be easy to use. Therefore, the level of effort required to adopt new aggregators should be minimal as well. Ultimately, the negligible efforts of adoption represent low customer switching cost.

All of the aforementioned characteristics are equally present in both industries, resulting in comparable bargaining power of buyers. Diluted buyers' power results from the large user base, insignificant volume of purchase, and low concentration of users. In contrast, the low switching cost increases the bargaining power of buyers. Even so, the overall buyer bargaining power is moderate for both industries. Hence, consumers have little influence on product development.

[240] OECD, "OECD Glossary of Statistical Terms - Sunk Costs Definition," accessed July 12, 2016, https://stats.oecd.org/glossary/detail.asp?ID=3317.

F. CONCLUSION

Based on Porter's Five Forces Framework analysis, leaders of the healthcare sector needs to modify its competitive forces to mimic that of financial services. The personal financial industry has a lower threat of new entrants and bargaining power of suppliers. These weaker forces result in more secure and interoperable products for consumers of financial account aggregators. On the contrary, the analysis reveals the opposite to be true for healthcare. Hence, healthcare industry's competitive forces need to be reshaped based best practices from the personal financial sector.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSION

This thesis concludes with recommendations, implementation strategies, limitations, and future research opportunities based on information and analyses presented in previous chapters. Recommendations aim to guide healthcare leaders to replicate best practices from the financial services industry. Implementation strategies include possible approaches to execute the proposed recommendations by forming a winning coalition. Finally, this chapter addresses study limitations and opportunities for future research.

A. RECOMMENDATIONS

The following recommendations focus on reshaping the healthcare industry's competitive forces to increase consumer benefits. These proposed changes are mainly derived from Porter's Five Forces Framework Analysis, which highlighted key distinctions between the healthcare and personal financial sectors. Three recommendations are suggested as possible ways to stimulate healthcare sector's transformation to more closely mirror that of financial services.

1. Fill the Gap in HIPAA

Participants of the quantified-self movement need security and privacy safeguards to protect their data and identities, respectively. Despite the overabundance of benefits associated with self-monitoring, quantified-self participants bear considerable risks as well. These risks include profiling by insurance companies, location tracking by criminals, extortion of victims, and corporate misuse of users' data.[241] Quantified-self participants should not be exposed to such vulnerabilities in exchange for their willingness to share personal health data for the greater good.

[241] Barcena, Wueest, and Lau, *How Safe Is Your Quantified Self?*, 20–21.

More comprehensive data security and privacy provisions are necessary to keep users from these potentially damaging impacts. As previously noted, legislation in the personal financial industry has no gaps in its security and privacy guidelines even with the introduction of account aggregators. This is not the case for the healthcare sector. While the FDA published new regulations for those designated as medical applications, the majority of quantified-self apps still lack basic security guidelines since HIPAA rules do not apply to user-generated health data.

The need to expand healthcare industry's legislative coverage is further supported by the analysis based on Porter's Five Forces Framework. The analysis in this thesis revealed that consumers benefit from personal financial sector's higher security and privacy standards. However, the gap in HIPAA's coverage would negatively impact users of healthcare aggregators. By filling in this gap, the healthcare leaders could better ensure the security and privacy of their users' information.

Yet, legislators should not stifle innovation with the establishment of baseline security and privacy requirements for healthcare aggregators. Even though the financial services sector has more comprehensive security legislation, regulators avoided adding unnecessary hurdles that might compromise technological advancement for users' benefits. These legislators value the balance between adequate security measures and industry growth. Correspondingly, policymakers could reapply this lesson to the healthcare sector by requiring only sufficient security and privacy standards to ensure consumer protection. Leaders of healthcare's emerging quantified-self movement should carefully navigate this delicate balance to prevent from unnecessarily suppressing innovation.

2. Encourage Industry Security Innovations

To advance towards personalized healthcare, developers need to focus on providing secure services for their users. The quantified-self movement

empowers users to be better informed in understanding and managing their health. Even though most quantified-self participants are willing to share their data, they also value the privacy of their identities and security of their data. The first recommendation serves as the initial attempt to reassure quantified-self participants of their information security. In addition, developers of healthcare aggregators should be encouraged to focus on innovating security and privacy solutions. These innovations could attract even the most wary users to aggregate and share their data.

As seen in the financial services industry, consumers would greatly benefit from aggregators' emphasis on innovative security solutions. Even though screen scraping is the most popular yet least secure method of aggregation, financial account aggregators have not reported any data breaches. Financial account aggregators go beyond the required security provisions, as exemplified by Mint's invitation for non-mandatory third-party audits. Most notably, Mint also invented and patented a pioneering security process to counter the main vulnerability of screen scraping. With these innovations, users could take advantage of the benefits from aggregation without having to be concerned about the security of their information. Therefore, leaders of the healthcare industry could adopt similar approaches to improve their industry's consumer benefits as well.

Furthermore, Porter's Five Forces Framework validated the consumer benefits of security innovations. The personal financial sector has a lower threat of new entrants with its inventive and extensive security processes. Development of original, or advanced, security measures helps to discourage inferior developers from entering the market. Such investments of time and effort represent added costs that would deter less qualified entrants. Also, exclusive security measures would differentiate financial account aggregators from substitutes such as Excel. Therefore, healthcare leaders need to concentrate on developing unconventional or cutting-edge security measures to encourage consumers to adopt these services.

3. Attract Third-Party Developers to Secure Data Interoperability

To reap the benefits of secure data aggregation and sharing, healthcare leaders need to focus on overcoming their industry's overarching interoperability issue. More specifically, device manufacturers and their associated apps often segregate users' data. While APIs enable data convergence, the effectiveness of this solution is impeded by the lack of interoperability efforts from corporations. Corporations block public access to their protocols and prevent their applications from integrating with apps of other firms. Furthermore, the industry's lack of standardization allows some databases to be more susceptible to hacking. These databases could become vulnerabilities to other apps or APIs that are connected. Therefore, industry leaders should focus on moderating corporate ownership so that data could be integrated and shared more securely.

In order to achieve secure integration, the healthcare industry could attract more third-party developers, mimicking the personal financial industry. Third-party developers, rather than banking institutions, produced most of the financial account aggregators. In contrast, healthcare device manufacturers also develop most of the leading aggregation apps and APIs. Therefore, these manufactures have less motivation and incentive to promote interoperability across devices or platforms. In contrast, third-party developers would prioritize the standardization of secure integration protocols.

As evident via the Porter's Five Forces Framework analysis, third-party developers could also increase consumer benefits for the healthcare sector by lowering its bargaining power of suppliers. Banks, as suppliers of financial account aggregators, have lower bargaining powers, because it is unlikely for them to offer aggregation services. However, device manufacturers, as suppliers of healthcare aggregators, have already taken on the additional role and launched many popular aggregation tools. Healthcare suppliers' success in forward integration could encourage others to follow suit. So, in order to stimulate interoperability, third parties should be encouraged to enter the healthcare industry. With motivations that align with consumer interests, third-party

developers might be more inclined to create standardized protocols for users to securely access their data across all barriers: apps, devices, and platforms.

B. IMPLEMENTATION STRATEGIES – BUILDING A WINNING COALITION

In this section, two possible implementation strategies for the first and second recommendations are explored. The first approach would be applicable to both recommendations, via the development of industry standards. The second approach would be to formalize the first recommendation with legislative changes. These two strategies are based on concepts from the *Dictator's Handbook*.

Building a winning coalition is the foundation for both implementation strategies. According to the *Dictator's Handbook*, there are three political groups: interchangeables, influentials, and essentials.[242] Leaders are encouraged to categorize people into these three fundamental groups in order to understand their political landscapes. Interchangeables, or nominal selectorates, are the largest group of potential supporters. A subset of interchangeables, influentials, is the real selectorate that truly drives leadership support. Lastly, essentials are the smallest subset of real and nominal supporters, who dictate leadership survival. Locating the essentials would be vital to the success of these implementation strategies as they are the essence of winning coalitions.

The third recommendation should transpire with the success of the first two. Once both recommendations are implemented, third-party interests should grow organically. Based on the conventional application of Porter's Five Forces Framework, the two recommendations should increase healthcare industry's profitability by lowering its threat of new entrants and bargaining power of suppliers. Profitable industries tend to attract prospective entrants; specifically, entrepreneurial new entrants drive industry growth via innovation. New entrants

[242] Bruce Bueno de Mesquita and Alastair Smith, *The Dictator's Handbook: Why Bad Behavior Is Almost Always Good Politics* (New York, NY: PublicAffairs, 2011), http://www.burmalibrary.org/docs13/The_Dictators_Handbook.pdf.

are more likely to invest in profitable industries, especially since innovation creates temporary monopolistic power and profits for the entrepreneurial firm.[243] The potential to become a temporary monopoly greatly incentivizes new firms to be creative. Innovation-led developments are crucial to industry growth. Hence, healthcare leaders need to ensure the success of the first two recommendations, as these changes would be necessary to yield a more favorable industry to attract entrepreneurial third parties.

1. Industry Standards

To avoid stifling innovation, healthcare industry's leaders could improve consumer benefits via industry standards. Standards Development Organizations (SDO) issue industry standards, which reflect industry professionals' opinion as to the "proper way to do or construct or connect a thing."[244] In essence, these standards are developed by industry experts as best practices based on their consolidated experiences. These published documents "maximize the reliability of the materials, products, methods, and/or services people use every day…[and] fuel the development and implementation of technologies that influence and transform the way we live, work and communicate."[245] Industry standards are one of the impactful ways to initiate change in industry practices.

To facilitate the establishment of industry standards based on recommendations from this thesis, industry leaders need to identify the three fundamental groups with respect to standards development. Since standards are derived from industry professionals, these experts are the interchangeables. Next, members of SDOs, as the influential, could contribute to standards development depending on SDO rules. Even though these two groups are large

---

[243] Gert-Jan Hospers, "Joseph Schumpeter and His Legacy in Innovation Studies," accessed July 9, 2016, https://www.researchgate.net/publication/225641651_Joseph_schumpeter_and_his_legacy_in_innovation_studies.

[244] Paul Grochowski, "Research Guides: Standards: About Industry Standards," accessed July 13, 2016, http://guides.lib.umich.edu/c.php?g=282907&p=1885163.

[245] IEEE, "IEEE-SA - Overview: What Are Standards?," accessed July 13, 2016, http://standards.ieee.org/develop/overview.html.

and less critical, sufficient efforts should be made to incorporate their opinions. Given the open involvement in standards development, support from these two groups still holds substantial weight in ensuring successful implementation. Within the SDO, dedicated working groups finalize, review, and approve draft standards, which are submitted for Sponsor balloting and then to the Review Committee and Standards Board. Thus, the winning coalition would require substantial representation at each step of the aforementioned process to ensure approval.

In order to form the winning coalition, healthcare leaders should create an alliance with technical SDO committee members. Two relevant SDO organizations are the Institute of Electrical and Electronics Engineers (IEEE) and International Organization for Standardization (ISO). IEEE is the "world's largest technical professional organization dedicated to advancing technology for the benefit of humanity."[246] ISO is "an independent, non-governmental international organization…[that] brings together experts to share knowledge and develop voluntary, consensus-based, market relevant International Standards that support innovation and provides solutions to global challenges." These two organizations have formed the ISO/IEEE Partner Standards Development Organization (PSDO) Cooperation Agreement to jointly develop international standards.[247] Both are mission driven to focus on technological advancements. These purpose-driven SDOs are less likely to compromise innovation in the process of standards development. Furthermore, the agreement includes health informatics as a key technical area committee, which looks to improve the healthcare system by facilitating exchange and use of health data and information.[248] Healthcare leaders should include members of this ISO technical

246 IEEE, "IEEE," accessed July 4, 2016, https://www.ieee.org/index.html.

247 IEEE, "IEEE-SA - Global Activities ISO," accessed July 13, 2016, https://standards.ieee.org/develop/intl/iso.html.

248 ISO, "ISO - Technical Committees - ISO/TC 215 - Health Informatics," *ISO*, accessed July 13, 2016, http://www.iso.org/iso/iso_technical_committee?commid=54960.

committee in their winning coalition in order to implement the first two recommendations from this thesis.

2. Legislative Change

Alternatively, once industry standards have demonstrated the success of these best practices, the first recommendation to fill the gap in HIPAA could be formalized via legislative changes. To identify the three political groups within this environment, healthcare leaders need to understand the legislative process. The following describes the procedure by which laws are processed:

> First, a representative sponsors a bill. The bill is then assigned to a committee for study. If released by the committee, the bill is put on a calendar to be voted on, debated or amended. If the bill passes by simple majority (218 of 435), the bill moves to the Senate. In the Senate, the bill is assigned to another committee and, if released, debated and voted on. Again, a simple majority (51 of 100) passes the bill. Finally, a conference committee made of House and Senate members works out any differences between the House and Senate versions of the bill. The resulting bill returns to the House and Senate for final approval. The Government Printing Office prints the revised bill in a process called enrolling. The President has 10 days to sign or veto the enrolled bill.[249]

Based on the procedure, interchangeables likely include all members of Congress. Subsequently, influentials would be the subset of representatives and senators necessary to reach a simple majority in both houses, 218 and 51, respectively. Finally, as essentials of the winning coalition, committee members would be responsible for releasing the bill for voting and lobbying for additional support to obtain the simple majority in the House and the Senate.

In particular, Representative Hank Johnson, a democrat from Georgia, would be a valuable member for the winning coalition. Representative Johnson introduced the Application Privacy, Protection and Security (APPS) Act in

[249] United States House of Representatives, "The Legislative Process: House.gov," accessed July 13, 2016, http://www.house.gov/content/learn/legislative_process/.

2013.[250] The Act seeks to protect users by requiring developers to notify them regarding the collection or sharing of users' information. It also deems developers responsible for securing users' data and identities. This Act seems to align closely with the proposed need for baseline security and privacy provisions.

In this case, growing the winning coalition is imperative. As of May 10, 2013, the bill has been referred to the House of Representative's Energy and Commerce Committee for their consideration.[251] It has gained the support of eight cosponsors as of July 31, 2014, including members from both the Democratic and Republican parties.[252] While the Act has obtained additional support since its introduction, it has yet to gain enough momentum to move the bill forward either to a subcommittee or a committee hearing. Therefore, healthcare leaders should continue to lobby for more substantial support, if they decide to pursue legislative changes.

C. RESEARCH LIMITATIONS

The research design of this thesis contains certain limitations within which the findings should be carefully interpreted. Some limitations to be considered include the data availability and lack of generalizability.

Selection of samples was constrained due to data availability. The case studies require detailed documentation on aggregators' technical capabilities and security measures. However, these documents are not always as readily available for the less popular aggregators. Therefore, this study mainly included well-known aggregators due to the limited availability of documentations.

Since this comparative study was conducted between specific aggregators from the two sectors, it might be difficult to generalize the findings to a broader range of products. This thesis simplified the focus aggregation technologies to

[250] Henry Johnson, "H.R.1913 –113th Congress (2013-2014): APPS Act of 2013," legislation, (May 10, 2013), https://www.congress.gov/bill/113th-congress/house-bill/1913.

[251] Ibid.

[252] Ibid.

applications, APIs, and screen scraping. Though these methods of aggregation are the widely used and commonly available, there are other methods that were not explored in this study. Hence, it might be difficult for policymakers, industry leaders, or consumers to extrapolate this thesis's research findings to other technologies.

D. FUTURE RESEARCH

Future research directions could focus on overcoming the limitations of this study and investigating the applicability of this thesis's findings to integration with EHR systems. With access to better documentations, sample selection would not need to be limited to the most popular aggregators. Additionally, more representative sampling would improve the generalizability of future research findings. To take this even further, researchers could conduct usage tests and surveys to determine the ideal technological features and security measures necessary to promote consumer participation. Lastly, while this study did not consider the interoperability of self-generated data with EHR, this integration would be crucial to the advancement towards personalized healthcare. As such, future research could place an emphasis on examining this aspect of the quantified-self movement.

LIST OF REFERENCES

Agrawal, Manish, Hemant Padmanabhan, Lokesh Pandey, H. R. Rao, and Shambhu Upadhyaya. “A Conceptual Approach to Information Security in Financial Account Aggregation.” In *Proceedings of the 6th International Conference on Electronic Commerce*, 619–26. ICEC ‘04. New York, NY: ACM, 2004. doi:10.1145/1052220.1052299.

Anderson, Catherine L., and Ritu Agarwal. “The Digitization of Healthcare: Boundary Risks, Emotion, and Consumer Willingness to Disclose Personal Health Information.” *Information Systems Research*, April 8, 2011. http://pubsonline.informs.org/doi/abs/10.1287/isre.1100.0335.

Apple Inc. “Apple - Press Info - Apple Advances Health Apps with CareKit.” Accessed April 17, 2016. http://www.apple.com/pr/library/2016/03/21Apple-Advances-Health-Apps-with-CareKit.html.

———. “Apple - Press Info - Apple Announces Advancements to ResearchKit.” Accessed April 17, 2016. http://www.apple.com/pr/library/2016/03/21Apple-Announces-Advancements-to-ResearchKit.html.

———. “HealthKit Framework Reference.” Accessed May 15, 2016. https://developer.apple.com/library/ios/documentation/HealthKit/Reference/HealthKit_Framework/.

———. “iOS 9 - Health.” Apple. Accessed April 18, 2016. http://www.apple.com/ios/health/.

———. “Use the Health App on Your iPhone or iPod Touch.” Apple Support. Accessed June 12, 2016. https://support.apple.com/en-us/HT203037.

Baldwin, Roberto. “Apple Updates HealthKit Privacy Policy to Ban Selling Data.” The Next Web, August 28, 2014. http://thenextweb.com/apple/2014/08/28/apple-updates-healthkit-privacy-rules-keep-health-data-hands-advertisers/.

Ballano Barcena, Mario, Candid Wueest, and Hon Lau. *How Safe Is Your Quantified Self?* Mountain View, CA: Symantec Corporation, August 11, 2014. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/how-safe-is-your-quantified-self.pdf.

Barr, Alistair. “Google’s New Moonshot Project: The Human Body.” *Wall Street Journal*, July 27, 2014, sec. Tech. http://www.wsj.com/articles/google-to-collect-data-to-define-healthy-human-1406246214.

Betterment. “Betterment Joint Accounts.” Accessed June 12, 2016. http://support.betterment.com/customer/portal/topics/749330-joint-accounts.

———. “Why Betterment.” Accessed May 30, 2016. https://www.betterment.com/why-betterment/.

Betters, Elyse, and Mike Lowe. “Apple ResearchKit and CareKit: Everything You Need to Know - Pocket-Lint,” March 21, 2016. http://www.pocket-lint.com/news/133132-apple-researchkit-and-carekit-everything-you-need-to-know.

BusinessWire. “What Do People Really Spend? Mint Data Delivers Real-Time View,” October 28, 2010. http://www.businesswire.com/news/home/20101028005921/en.

———. “ResearchKit at 6 Months: 100,000 People Now Using Medical Apps,” October 15, 2015. http://www.macworld.com/article/2993838/ios/researchkit-at-6-months-100-000-people-now-using-medical-apps.html.

CareKit. “Overview Document.” Accessed June 13, 2016. http://carekit.org/docs/docs/Overview/Overview.html.

Dachis, Adam. “Sherbit Visualizes and Interprets All the Data Your Online Services Collect.” Lifehacker. Accessed June 12, 2016. http://lifehacker.com/sherbit-visualizes-and-interprets-all-the-data-your-onl-1779567985.

Diamond, Carol C., Farzad Mostashari, and Clay Shirky. “Collecting And Sharing Data For Population Health: A New Paradigm.” *Health Affairs* 28, no. 2 (March 1, 2009): 454–66. doi:10.1377/hlthaff.28.2.454.

Doukas, C., I. Maglogiannis, V. Koufi, F. Malamateniou, and G. Vassilacopoulos. “Enabling Data Protection through PKI Encryption in IoT M-Health Devices.” In *2012 IEEE 12th International Conference on Bioinformatics Bioengineering (BIBE)*, 25–29, 2012. doi:10.1109/BIBE.2012.6399701.

Economist, The. “Cracking the Vault.” *The Economist*, October 24, 2015. http://www.economist.com/news/finance-and-economics/21676826-grip-banks-have-over-their-customers-weakening-cracking-vault.

Evans, Jonny. “How to Export Apple Health Data as a Document to Share.” Accessed June 12, 2016. http://www.computerworld.com/article/2889310/how-to-export-apple-health-data-as-a-document-to-share.html.

Federal Reserve. “Federal Trade Commission Act Section 5: Unfair or Deceptive Acts or Practices.” Consumer Compliance Handbook, June 2008. https://www.federalreserve.gov/boarddocs/supmanual/cch/ftca.pdf.

Federal Trade Commission. “FTC Releases New Guidance For Developers of Mobile Health Apps.” Accessed April 20, 2016. https://www.ftc.gov/news-events/press-releases/2016/04/ftc-releases-new-guidance-developers-mobile-health-apps.

———. “Mobile Health App Developers: FTC Best Practices.” Accessed April 20, 2016. https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-app-developers-ftc-best-practices.

FFIEC. “FFIEC IT Examination Handbook InfoBase - Appendix D: Aggregation Services.” Accessed January 22, 2016. http://ithandbook.ffiec.gov/it-booklets/e-banking/appendix-d-aggregation-services.aspx.

FreshBooks. “FreshBooks Cloud Accounting.” Accessed August 8, 2016. https://www.freshbooks.com/expenses-and-receipts-tracking.

Fujii, Hiroshi, Taeko Okano, Stuart Madnick, and Michael Siegel. “E-Aggregation: The Present and Future of Online Financial Services in Asia-Pacific.” SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, July 1, 2002. http://papers.ssrn.com/abstract=376864.

Gay, Valerie, and Peter Leijdekkers. “Bringing Health and Fitness Data Together for Connected Health Care: Mobile Apps as Enablers of Interoperability.” *Journal of Medical internet Research* 17, no. 11 (November 18, 2015). doi:10.2196/jmir.5094.

GitHub. “ResearchKit/ResearchKit.” Accessed May 30, 2016. https://github.com/ResearchKit/ResearchKit.

Google Fit. “Terms and Conditions.” Google Developers. Accessed May 15, 2016. https://developers.google.com/fit/terms.

Graziano, Dan. “The Complete Guide to Google Fit.” *CNET*. Accessed April 18, 2016. http://www.cnet.com/how-to/the-complete-guide-to-google-fit/.

Grochowski, Paul. “Research Guides: Standards: About Industry Standards.” Accessed July 13, 2016. http://guides.lib.umich.edu/c.php?g=282907&p=1885163.

Hackett, John. “Domesticating Account Aggregators.” American Banker. Accessed June 5, 2016. http://www.americanbanker.com/btn/13_10/-135131-1.html.

Harry, Rhodes. “Accessing and Using Data from Wearable Fitness Devices” 85, no. 9 (September 2014): 48–50.

Health Information & the Law. “Fast Facts.” healthinfolaw.org, August 2015.

Hospers, Gert-Jan. “Joseph Schumpeter and His Legacy in Innovation Studies.” Accessed July 9, 2016. https://www.researchgate.net/publication/225641651_Joseph_schumpeter_and_his_legacy_in_innovation_studies.

IEEE. “IEEE.” Accessed July 4, 2016. https://www.ieee.org/index.html.

———. “IEEE-SA - Global Activities ISO.” Accessed July 13, 2016. https://standards.ieee.org/develop/intl/iso.html.

———. “IEEE-SA - Overview: What Are Standards?” Accessed July 13, 2016. http://standards.ieee.org/develop/overview.html.

IFTTT. “IFTTT.” *IFTTT / Connect the Apps You Love.* Accessed August 8, 2016. https://ifttt.com/.

———. “Tweet When You Achieve Your Daily Fitbit Step Goal.” IFTTT / Connect the Apps You Love. Accessed August 8, 2016. https://ifttt.com/recipes/175106-tweet-when-you-achieve-your-daily-fitbit-step-goal.

Imgur. “Imgur: The Most Awesome Images on the internet.” Imgur. Accessed June 12, 2016. http://imgur.com/TbSKGAl.

Institute for Critical Infrastructure Technology. “Hacking Healthcare IT in 2016,” January 2016. http://icitech.org/wp-content/uploads/2016/01/ICIT-Brief-Hacking-Healthcare-IT-in-20161.pdf.

ISO. “ISO - Technical Committees - ISO/TC 215 - Health Informatics.” *ISO*. Accessed July 13, 2016. http://www.iso.org/iso/iso_technical_committee?commid=54960.

Johnson, Henry. “H.R.1913 - 113th Congress (2013-2014): APPS Act of 2013.” Legislation, May 10, 2013. https://www.congress.gov/bill/113th-congress/house-bill/1913.

Keivani, F. Sameni, M. Joubarkand, and M. Khodadadi. “A General View on E-Banking.” Roudsar, Iran: Department Accounting, Islamic Azad University, Roudsar and Amlash Branch, n.d.

Kessler, Tim, Christoph Buck. “Mobile Consumer Apps: Big Data Brother Is Watching You.” *Marketing Review St. Gallen* 31, no. 1 (2014): 26–35. doi:10.1365/s11621-014-0318-2.

Lanks, Belinda. “The Quantified Self: How Cold, Hard Data Improve Lives.” *Bloomberg.com*. Accessed May 1, 2016. http://www.bloomberg.com/news/features/2015-03-27/the-quantified-self-how-cold-hard-data-improve-lives.

Luke Landes. “Mint.com Tracks Two Million Users to Create Spending Index.” Accessed June 11, 2016. http://www.consumerismcommentary.com/mint-intuit-consumer-spending-index/.

Majmudar, Maulik D., Lina Avancini Colucci, and Adam B. Landman. “The Quantified Patient of the Future: Opportunities and Challenges.” *Healthcare (Amsterdam, Netherlands)* 3, no. 3 (September 2015): 153–56. doi:10.1016/j.hjdsi.2015.02.001.

Makary, Martin A., and Michael Daniel. “Medical Error—the Third Leading Cause of Death in the US.” *BMJ* 353 (May 3, 2016): i2139. doi:10.1136/bmj.i2139.

Marketwired. “New Ovum Study Looks at API Security Practices, Revealing Basic Security Measures and Attack Vectors Overlooked and Disconnect Between Developers and IT Security Teams.” *Yahoo Finance*. Accessed June 12, 2016. http://finance.yahoo.com/news/ovum-study-looks-api-security-130000389.html.

Max. “Best Digital Health System: Google Fit vs. Apple HealthKit.” Appcessories, App-Enabled Accessories and Wearables, November 27, 2015. http://www.appcessories.co.uk/the-best-digital-health-system-google-fit-vs-apple-healthkit/.

Mearian, Lucas. “By 2020, There Will Be 5,200 GB of Data for Every Person on Earth.” *Computerworld*, December 11, 2012. http://www.computerworld.com/article/2493701/data-center/by-2020--there-will-be-5-200-gb-of-data-for-every-person-on-earth.html.

Mesquita, Bruce Bueno de, and Alastair Smith. *The Dictator’s Handbook: Why Bad Behavior Is Almost Always Good Politics*. New York, NY: PublicAffairs, 2011. http://www.burmalibrary.org/docs13/The_Dictators_Handbook.pdf.

McGarry, Caitlin. “Apple’s CareKit Gives You and Your Doctors a Better Understanding of Your Health.” *Macworld*, March 21, 2016. http://www.macworld.com/article/3046513/software/apples-carekit-gives-you-and-your-doctors-a-better-understanding-of-your-health.html.

Michaels, David. United States Patent: 8566952 - System and method for encrypting data and providing controlled access to encrypted data with limited additional access. 8566952, issued October 22, 2013. http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PALL&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.htm&r=1&f=G&l=50&s1=8,566,952.PN.&OS=PN/8,566,952&RS=PN/8,566,952.

Mint. “4 Things You Didn’t Know a Budget App Could Do.” Mint, October 7, 2013. https://www.mint.com/budgeting-apps/4-things-you-did-not-know-a-budget-app-could-do.

———. “All in One.” Mint. Accessed February 21, 2016. https://www.mint.com/.

———. “Mint Bills Privacy and Security.” Mint, May 7, 2015. https://www.mint.com/mintbills/mobile/privacy_and_security.

Moeller, Philip. “How to Track All Your Money From One Place.” U.S. *News & World Report*, May 24, 2013. http://money.usnews.com/money/blogs/the-best-life/2013/05/24/how-to-track-all-your-money-from-one-place.

NBC News. “What It Was Like Before ATMs and Online Banking.” NBC News. Accessed June 4, 2016. http://www.nbcnews.com/video/what-it-was-like-before-atms-and-online-banking-472991811754.

Nield, David. “Google Fit v Apple Health.” Wareable. Accessed May 15, 2016. http://www.wareable.com/sport/google-fit-vs-apple-health.

OECD. “OECD Glossary of Statistical Terms - Sunk Costs Definition.” Accessed July 12, 2016. https://stats.oecd.org/glossary/detail.asp?ID=3317.

Office for Civil Rights. “Summary of the HIPAA Privacy Rule.” Text. HHS.gov, May 7, 2008. http://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

Office of the Chief Accountant. “Audit Committees and Auditor Independence.” U.S. Securities and Exchange Commission, April 27, 2007. https://www.sec.gov/info/accountants/audit042707.pdf.

Office of the Comptroller of the Currency. “Bank-Provided Account Aggregation Services: Guidance to Banks,” February 28, 2001. http://www.occ.gov/news-issuances/bulletins/2001/bulletin-2001-12.html.

Office, U.S. Census Bureau Public Information. “Americans Are Visiting the Doctor Less Frequently, Census Bureau Reports - Health Care & Insurance - Newsroom - U.S. Census Bureau.” Accessed May 1, 2016. https://www.census.gov/newsroom/releases/archives/health_care_insurance/cb12-185.html.

Personal Capital. “Financial Planning Software & Finance Apps.” Accessed April 16, 2016. https://www.personalcapital.com.

———. “Free Finance Tools, Calculators & Software.” Accessed April 14, 2016. https://www.personalcapital.com.

Michael E. Porter. *Competitive Strategy: Techniques for Analyzing Industries and Competitors: With a New Introduction*. New York, NY: The Free Press, 1998. http://www.vnseameo.org/ndbmai/CS.pdf.

———. “How Competitive Forces Shape Strategy.” *Harvard Business Review*, March 1, 1979. https://hbr.org/1979/03/how-competitive-forces-shape-strategy.

———. “The Five Competitive Forces That Shape Strategy.” *Harvard Business Review*, January 2008, 79–93.

Price, Emily. “10 Things You Didn’t Know Mint Could Do.” Mashable. Accessed April 15, 2016. http://mashable.com/2012/08/22/mint-tips/.

Proffitt, Brian. “What APIs Are And Why They’re Important.” ReadWrite, September 19, 2013. http://readwrite.com/2013/09/19/api-defined/.

Qualcomm Tricorder XPrize. “Overview.” Qualcomm Tricorder XPRIZE, September 11, 2015. http://tricorder.xprize.org/about/overview.

QuickMBA. “Porter’s Five Forces.” Accessed June 25, 2016. http://www.quickmba.com/strategy/porter.shtml.

Ramirez, Ernesto. “How to Download Minute-by-Minute Fitbit Data.” Quantified Self, September 26, 2014. http://quantifiedself.com/2014/09/download-minute-fitbit-data/.

Razzouk, Nadine. “Quantified Self,” 2015. http://ft.parsons.edu/skin/wp-content/uploads/2015/05/Nadine_RAZZOUK1.pdf.

Roth, Marc S., and Charles Washburn. “Data Brokers Face Blurring Lines, Increased Regulatory Risks.” Accessed June 5, 2016. http://www.bna.com/data-brokers-face-blurring-lines/.

Saranow Schultz, Jennifer. “Should You Trust Mint.com?” *New York Times*. Accessed February 7, 2016. http://bucks.blogs.nytimes.com/2010/07/06/should-you-trust-mint-com/?_r=0.

Schooner, Heidi Mandanis, and Michael Taylor. “United Kingdom and United States Reponses to the Regulatory Challenges of Modern Financial Markets.” *Texas International Law Journal* 38 (2003): 317.

Schultz, Jennifer Saranow. “Should You Trust Mint.com?” *Bucks Blog*, 1278443106. http://bucks.blogs.nytimes.com/2010/07/06/should-you-trust-mint-com/.

Scott, Johanna. “New Integration with Mint.” Betterment, November 16, 2011. https://www.betterment.com/resources/inside-betterment/new-integration-with-mint/.

Shameer, Khader, Marcus A. Badgeley, Riccardo Miotto, Benjamin S. Glicksberg, Joseph W. Morgan, and Joel T. Dudley. “Translational Bioinformatics in the Era of Real-Time Biomedical, Health Care and Wellness Data Streams.” *Briefings in Bioinformatics*, February 14, 2016, bbv118. doi:10.1093/bib/bbv118.

Sherbit. “About.” Sherbit-Personal Analytics. Accessed May 15, 2016. https://www.sherbit.io/about/.

———. “Sherbit Privacy Policy.” Sherbit- Personal Analytics. Accessed May 14, 2016. https://www.sherbit.io/privacypolicy/.

Spiotto, Ann S. “Financial Account Aggregation: The Liability Perspective.” *Fordham Journal of Corporate & Financial Law* 8, no. 2 (2003): 557–605.

Stack Exchange Inc. iIcloud - View iOS Health Data Externally - Ask Different.” Accessed July 12, 2016. http://apple.stackexchange.com/questions/167671/view-ios-health-data-externally.

Stalter, Kate. “The Future of Banking.” Accessed June 4, 2016. http://money.usnews.com/money/personal-finance/articles/2015/06/29/the-future-of-banking.

Stanford University. “An Introduction to Philosophy.” Accessed August 8, 2016. https://web.stanford.edu/~bobonich/dictionary/dictionary.html.

Swan, Melanie. “Sensor Mania! The internet of Things, Wearable Computing, Objective Metrics, and the Quantified Self 2.0.” *Journal of Sensor and Actuator Networks* 1, no. 3 (November 8, 2012): 217–53. doi:10.3390/jsan1030217.

———. “The Quantified Self: Fundamental Disruption in Big Data Science and Biological Discovery.” *Big Data* 1, no. 2 (June 1, 2013): 85–99. doi:10.1089/big.2012.0002.

Tai-Seale, Ming, Thomas G McGuire, and Weimin Zhang. “Time Allocation in Primary Care Office Visits.” *Health Services Research* 42, no. 5 (October 2007): 1871–94. doi:10.1111/j.1475-6773.2006.00689.x.

Team FME. *Porter’s Five Forces*. www.free-management-ebooks.com, 2013. http://www.free-management-ebooks.com/dldebk-pdf/fme-five-forces-framework.pdf.

Teusink, Joram. “Android Wear and Google Fit and Its Privacy and Security ~ Teusink.” Accessed January 25, 2016. http://www.teusink.eu/2015/02/android-wear-and-google-fit-security-privacy.html.

Till, Chris. “Exercise as Labour: Quantified Self and the Transformation of Exercise into Labour.” *Societies* 4, no. 3 (August 28, 2014): 446–62. doi:10.3390/soc4030446.

TRUSTe. “TRUSTe History - Nearly Two Decades of Privacy Innovation.” *TRUSTe*. Accessed May 14, 2016. https://www.truste.com/about-truste/company-history/.

United States House of Representatives. “The Legislative Process: House.gov.” Accessed July 13, 2016. http://www.house.gov/content/learn/legislative_process/.

U.S. Department of Health and Human Services, Food and Drug Administration, Center for Devices and Radiological Health, and Center for Biologics Evaluation and Research. “Guidance for Industry and Food and Drug Administration Staff.” Food and Drug Administration, February 9, 2015. http://www.fda.gov/downloads/MedicalDevices/.../UCM263366.pdf.

U.S. Department of Health and Human Services, Office for Civil Rights. “HIPAA Administrative Simplification,” March 26, 2013. http://www.hhs.gov/sites/default/files/hipaa-simplification-201303.pdf.

Verisign, Inc. “Verisign, Inc. Is A Leader In Domain Names And internet Security - Verisign.” Accessed May 14, 2016. https://www.verisign.com/.

Wei, Jie, and Jing Zhao. “Pricing Decisions for Substitutable Products with Horizontal and Vertical Competition in Fuzzy Environments.” *Annals of Operations Research*, February 4, 2014, 1–24. doi:10.1007/s10479-014-1541-6.

Wessel, David. “The Hutchins Center Explains: How Blockchain Could Change the Financial System (part 1).” The Brookings Institution. Accessed June 4, 2016. http://www.brookings.edu/blogs/up-front/posts/2016/01/11-how-blockchain-change-financial-wessel.

Wierzel, Kimberly. “If You Can’t Beat Them, Join Them: Dara Aggregators and Financial Institutions.” *North Carolina Banking Institute* 5, no. 1 (April 1, 2001): 457.

Williams, Julie L. “The Impact of Aggregation on the Financial Services Industry,” 1–7. Tysons Corner, Virginia: Administrator of National Banks, 2001. http://www.occ.gov/static/news-issuances/news-releases/2001/nr-occ-2001-39.pdf.

Wong, Kristin. “How to Start Tracking Your Investments With Personal Capital.” Two Cents. Accessed May 30, 2016. http://twocents.lifehacker.com/how-to-start-tracking-your-investments-with-personal-ca-1697801188.

Yang, Y. Tony, and Ross D. Silverman. “Mobile Health Applications: The Patchwork Of Legal And Liability Issues Suggests Strategies To Improve Oversight.” *Health Affairs* 33, no. 2 (February 1, 2014): 222–27. doi:10.1377/hlthaff.2013.0958.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California