Max Patten
December 9th, 2021
Professor Ali
MDST 4510: Political Economy of Communication

The Political Economy of Apple Devices and Valuable User Data

Introduction

As I look through my iPhone, a pleasant selfie of my girlfriend and I on vacation is suggested on my home screen. I tap to see that I can further tap into my face, hers, or that of my sister, mom, and friends to see indexed collections of close people in my life. Curious to see how my training is going, I swipe into the Health app to see sleep tracking and idle/active heart rate data from the last week of my life. Bored with my surroundings, I ask Siri to put on one of my favorite playlists before noticing my AirPods are missing. A quick tap into the Find My app reveals I left them behind at home, so I turn around to hurry back and grab them. Looking at the Watch on my wrist, I decide to track this run and see what my mile pace is. Apple tells me "privacy is a fundamental human right," (Apple, Platform Security, 6) and that they are committed to keeping data securely on my devices. But what does it mean that all this data — much of it invaluable and irreplaceable to me — is on my devices in the first place?

In recent years, scandal after scandal seems to surround social media firms and tech giants once regarded as infallible. Particular attention has been paid to companies like and Google whose businesses are structured off online services and lucrative data scraped from their respective ubiquity in social media and search online. Less scrutiny has been directed to Apple, the massive consumer electronics company whose devices are adored by users and the mainstream media. "What happens on your

iPhone stays on your iPhone" (Hacgman, *IDG*) read a recent billboard campaign run by the company. The company repeatedly fashions itself as an emblem of "privacy leadership" (Apple) in press releases. When four Big Tech CEOs were called in front of Congress in 2020, an Associated Press release at the time addressed how "[Apple CEO] Cook drew less attention from lawmakers than did the other CEOs." (Liedtke et al, *AP Business*). A management consulting executive advising AP Business said that Apple's polished CEO delivered "a master class in terms of how to handle these situations." It seems as if the spotlight of public and academic scrutiny surrounding Big Tech has left Apple and its ubiquitous products largely unexposed.

As Apple's success has blossomed in the wake of iPhone's ubiquity its products have asserted more control over their users. Apple devices collect reliable and sensitive streams of data through increasingly personal and intimate channels like an always-on assistant, background photo scanning, and the world's most successful wearable product. Data-based features like Siri, iCloud, and a proprietary lost-device network keep users coming back to Apple devices with their sticky utility. While it is tempting to categorize Apple as a firm chiefly in the business of luxury consumer electronics, the quantity of information that flows from and through its devices makes its involvement in data hard to ignore. While the firm does notably design secure systems, it also continues to push the edges of *what* data gets collected with its ever-more capable products. The secure systems it innovates are also locked down and under a tight grip of integration. Through a very tangible basis of hardware sensors and proprietary software spread over billions of overall devices, Apple products are an

opaque, yet sacred home for their users' data. This quantification at a massive scale should not be dismissed as trivial.

Wishing to become more of a "health company" (Gurdus, *CNBC*) according to CEO Tim Cook, Apple is betting on being an even more instrumental part of its users' lives going forward. Already, Apple Watch continuously measures people's heart rates and records their location from their wrists, Siri hears unfathomable amounts of voice recordings every day, and wireless data shared between iDevices flood the world's airwaves with proprietary and mysterious protocols. Apple is still thought of as a hardware vendor; but it is impossible to ignore the firm's growing role in trafficking and directing massive quantities of global information from its billions of increasingly capable and sensitive devices. This paper is an exercise in waking up to the material consequences of Apple's control over myriad user data in the design of its products and the features it markets them with.

Research Questions and Methods

The research questions focus on the specifics of Apple's data collection efforts, documenting instances where Apple controls the flow of user data or plays a role in aggregating it. As the vendor of both hardware and software blended into seamless products, Apple enjoys a unique position of integrated control over its users compared to more discrete and less integrated companies, like Samsung or Microsoft, who are known primarily as hardware or software firms respectively. The firm's billions of globally distributed devices inform its relationship to users. While users own Apple

devices through purchasing them, they also must use Apple's proprietary software stack built into their devices. Additionally, I ask what financial or power-related incentives does Apple — regardless of its public messaging — have in collecting and maintaining control over the highly sensitive information of its users?

Investigating these research questions involves specific examples of Apple leveraging control over its users and documented types of data collected in these relationships and scenarios. The research questions address the value of the data users generate and transmit through Apple devices and features. The primary sources will involve official documentation by the company itself on its integrated product features like Siri and photo-scanning, as well as academic studies and articles surrounding products like Apple Watch. These features and products serve as case studies for the company's control of user data. Studies from law, health science, computer science, and sociology provide a diverse and balanced view of the information opportunities and threats in Apple's integrated products from multiple disciplines. I also employ occasional firsthand, ethnographic data as an Apple user who is heavily invested in the company's ecosystem.

Background and Literature Review

While Apple emphasizes services as an area of growth to investors, the bulk of its net sales still come from hardware products like iPhone, iPad, and Apple Watch — nearly 89 percent per the company's Q1 2021 earnings report. Apple is still by and large a hardware business, but why is its hardware so tenaciously successful? While

the hardware is excellent; much of the features and utility of devices comes from data. My literature and case studies illustrate the importance of user-based data to Apple's keystone products and the role of data in value-adding features like Find My and Siri. Rather than suggesting malfeasance with handling of data or intrusive surveillance, the examples and studies cited lay out myriad situations where Apple tightly controls user data and criticize failures to disclose or make transparent the abundance of information Apple collects. Much of this information is either sensitive or highly valued by users, from biometric readings like heart rate to location data or photos of loved ones. The studies point out instances where this data can be commodified or where the mere control of it can add significant value to Apple's devices.

The "Who Can Find My Devices" article by Heinrich et al. is a technical analysis of Apple's Find My system which is instrumental to citing how the location-tracking system works in my paper. Its technical detail and computer science-oriented language make it a rich example of security experts dissecting and critiquing an Apple service that relies on location data shared across hundreds of millions of devices. The researchers notably failed to find "ample proof for [Apple's] claims" about privacy due to the undocumented nature of its proprietary implementation. This is a black box not only for users, but for security researchers who are responsibly identifying and disclosing privacy bugs in the system. The circumstances of this research and the frustrations of the writers is a key example of Apple asserting control and lacking transparency in its protocols for data exchange.

Candice Lanius' "Rhetorical Implications of Contract Tracing Mobile Applications" takes aim at Apple and Google's joint effort to fight the COVID-19 pandemic. While not the same implementation as Find My, the technology is built on similar building blocks and sees two Big Tech players that represent a smartphone oligopoly working together. Echoing communication scholars like Vincent Mosco, Lanius' argument criticizes the "big data solution" to what is fundamentally a social health issue. Lanius questions the tech solution by pointing out how people don't always carry location-tracking smart devices with them, de-normalizing an assumption that Apple is all too happy to make with its users. The implied rhetoric in tech-marketing is that users are always-on; always ready to use the next app or feature to make their lives better. The instance of contact-tracing sees Apple using aggregated user data to present a solution to the public. The criticism centers around using devices as proxies for people in virology, an assumption built into Apple and Google's design which Lanius finds ineffective and misleading.

Wayne et al.'s publication on "The Role of Artificial Intelligence and Data Network Effects for Creating User Value" thoughtfully examines the technology of artificial intelligence on devices like iPhone and connects the tech to user retention. With its description of data as "oil" for the digital economy and mention of the "network effect" from a software engineering perspective, the researchers explicitly connect user data to value added to devices. Be it in the cloud or on-device, this paper argues, data fed to Siri makes products like iPhone smarter and more convenient for users. The argument is not that Siri and artificial intelligence are necessarily detrimental to user

privacy, but that their ubiquity in Apple's operating system is key to differentiating Apple products from competition. The firm sells users not just devices, but over time, access to a personalized experience. The more users participate in data exchange with Apple devices, the more value unique to Apple devices they generate. This data is not transferable or easily visible in iOS. The suggestion is that users are participating in their own dependence on Apple software through training their devices to their habits and preferences.

Clancy et al.'s focus on Apple Watch in "Work and Play with the Apple Watch" is a thoughtful dissection of Apple's marketing message around the Watch in practice. It sees a fun gadget that strives to make "positive user experiences" yet also threatens to introduce work life into leisure and thus confirm the fears of media scholars like Dallas Smythe. The researchers posit that the excitement users get feeding data into the Watch "is really just another repetitive mindless task in 'ultramodern getup.'" (Clancy et al., 85) The work is auto-ethnographic and thus not experimentally rigorous in its data pool; it is useful because it presents at technologically optimistic view of the Watch while introducing issues and criticisms around how the health and data-tracking capabilities of the device might have social consequences which parallel concerning trends in information capitalism. The article is a convenient illustration of both data affordances and vulnerabilities embedded in the design of Apple Watch. Beyond being a neat gadget, Apple Watch derives value from the user data it captures and stores.

Grant Arnow's legal-oriented "Apple Watch-Ing You: Why Wearable Technology Should Be Federally Regulated" contrasts the robust enforcement of HIPAA in standard

medical practice with the lack of that scrutiny onto digital portals for healthcare — namely wearable products. There is also mention of frequent information breaches and poor information security practices in institutions and hospital systems, outlining the risks present when healthcare embraces commodified technology without the scrutiny of traditional medical security to back it up. It excellently captures the threat of Apple Watch as a device that is advertised for medical and health-oriented purposes while eluding regulatory and public scrutiny. The author does assume that "access to patients through wearable devices" is a boon for healthcare, a statement I would qualify and criticize, but industry-specific qualifications of the author make their arguments nonetheless useful for connecting wearable data to health regulation.

Apple's privacy documentation for its Photos app details how machine learning applied to user photos enables a convenient and curated library experience, allowing users to simply type in search terms and identify photos with specific "scenes … people and pets" as well as have photos suggested to them based on "quality analysis" ranking that considers factors like composition, lighting, and environmental audio for Live Photos and videos. While Apple stresses that the feature is on-device and not shared to iCloud or third parties, it also markets the degree to which the feature is "optimized for Apple devices," enabled by custom processors and machine-learning models whose designs are safeguarded industry secrets. Users must take Apple at their word that the most fundamental elements of its products are designed with security, because the devices' inner-workings are inscrutable and mysterious at their core. The primary source depicts how Apple's integration of data

into its devices enables it to market features, all while handling sensitive photos which are most conveniently backed up to iCloud and viewed on Apple's own devices. As with the case of Siri and on-device intelligence, users increasingly depend on Apple in everyday life at the cost of data independence, or for instance the possibility of switching platforms. Their data is alienated through the mystique of Apple integration.

Case Studies and Findings

The Apple Watch is arguably the most successful wearable hardware and is sold to users as a transformative health device. The "quantified self" nature of Apple Watch directly connects the philosophies of Big Data, as defined by media scholar Vincent Mosco in his book *Becoming Digital: Toward a Post-Internet Society*. Mosco argues that the "quantified self" as a concept is reinforced in "the growing tendency to focus on quantitative readings of bodily activities." (Mosco, 102) Apple Watch is marketed as a productive health product — it happens to regularly collect heart rate, tracks physical activities like running routes, and maps location over GPS. Health insurance companies like Aetna have jumped at the opportunity to develop programs for patients that "offer personalized goals*, achievable actions and big rewards** — like an Apple Watch or gift cards from popular retailers." (Aetna) A connection can be made from the quantified self which Mosco discusses to a commodified identity embodied by data from the self. Businesses like health insurance depend on data to evaluate quotes and cover their patients; thus the Watch is an enviable data platform on which to build and help promote. While Apple is keen to emphasize its privacy-preserving design of its Health

app on its healthcare promotional page, the centralization of health records and biometric data from Apple Watch into an Apple-controlled app call into question what the firm might gain from its expansion into wellness.

A provocative think piece from Computerworld mentions Apple's partnerships with both health insurance firms and large employers like IBM who have large wellness programs encouraging employees to wear an Apple Watch, leading to "reduced company health insurance premiums as insurers charge less for healthier habits." (Evans, *Computerworld*) Evans suggests that "without safeguards around privacy and fair use of information gathered by these systems, it is conceivable employers will eventually track every move their employees make." Social-oriented studies similarly show concern with health data, questioning how the Watch might be "offering opportunities to merge leisure and labour" (Wilmott, Fraser, et al.) as an always-on, novelty tech device that "demand[s] constant attentiveness" from previously unquantified interactions. The Loyola Law Review article on medical privacy and wearables warns "because wearable technology is new, and evolving rapidly, its innovation eclipses the existing regulatory framework and outpaces the legislative process." (Arnow 609) Apple Watch is fun and impressive as a health device; but it also invites a whole new stream of biological and sensitive data into the grasp of not only Apple, but the privatized healthcare system that Apple mutually works with. The company can say all it wants about privacy, but legal frameworks like HIPAA have not caught up to enforce digital health data as robustly as the real world. The Apple Watch as a health product has the firm partnering with the insurance and healthcare industries

to manage people's well-being; Apple is incentivized to work with these profit-maximizing and data-hungry industries because they help it sell more Apple Watches.

The Apple Watch is one of many location-enabled Apple mobile products participating in a proprietary "Find My" network, which leverages GPS and Bluetooth on devices like the Watch and iPhone to construct a global network of devices linked to each other by both precise location data and calculated proximity. Apple has been careful to highlight the privacy-oriented design of this network but has also not been shy about marketing the feature to users as a way of easily recovering lost goods. Extending this network beyond its own hardware, Apple's AirTag is a low-cost product sold to users as a way of making dumb things, like a wallet or luggage, "smart" and location aware. The system "works offline by sending out short range Bluetooth signals from the missing device that can be detected by other Apple devices in use nearby." (Apple, 161). A peer-reviewed security study on the Find My system had to reverse-engineer the system to expose and report privacy bugs to Apple, expressing a desire for Apple "to provide not only partial [6] but complete documentation of their systems and release components as open-source software whenever possible." (Heinrich et al., 242) Apple's secretive implementation of offline finding is a roadblock to true transparency and assessment of the company's ambitious claims to privacy. Additionally, the Find My network's management by Apple has raised antitrust concerns about ecosystem power from small competitors like lost item finder Tile, whose CEO criticized Apple considering the firm's "well-documented history of using

its platform advantage to unfairly limit competition for its products." (Prober quoted per Perez, *Engadget*) While Find My is open to third parties, Apple's gesture suggests it plans to dominate the market with its proprietary method due to the massive scale of iPhone users using the built-in solution.

A similar tracking technology has been employed by Apple and Google in the service of contact-tracing during the COVID pandemic; the assumption being that users carry their devices with them everywhere and that thus, electronic devices can inform and suggest the dynamics of real-world phenomena like transmissible diseases. The behavior of constantly being tracked is normalized through these kinds of marketed benefits. A rhetorical examination of these contact tracing methods suggests "opening our bodies to be sensed by these networked systems" (Lanius, 1) might not lead to successful outcomes, but rather "reveal the uncomfortable truth about many big data technologies: the promised benefits and myth of a data-driven, technologically empowered utopian society are not here and may never arrive." (16) Beyond Lanius, health officials have called the feature "practically useless." (Albergotti and Harwell, *The Washington Post*) Proponents of the technology blamed "outdated privacy laws" for "doomed contact-tracing apps." (Rich, *Brookings*) Regardless, in media and health circles even the most generous assessments of Apple and Google's joint effort suggest mixed results. Apple on its Health page described its effort as "crafting technical tools to help combat the virus and save lives," using its reputation as a privacy-oriented tech company to normalize carrying around Bluetooth smart-devices everywhere — a necessary assumption for a contact-tracing solution as proposed to work. If the effort

was a failure, tech would suggest that humans just haven't caught up enough to let the *deus ex machina* solve the world's problems. In connecting technology to noble pursuits like saving lives, Apple and other promoters present their solution as an intrinsically beneficial one.

In yet another recent example of always-on normalization, media outlets like POLITICO lampooned Vice President Kamala Harris for being skeptical of Bluetooth headphones and accessories, calling her "Blueooth-phobic" and inviting a "snark-a-thon" (Bixby et al, *The Daily Beast*) on social media. While not explicitly related to location information, Harris' concerns tap into well-documented security issues with the technology. The NSA even released a document on data exposure through Bluetooth, alerting citizens that their location and device data can be shared even with cellular off through bad-actor Bluetooth connections that can leverage their connection to obtain data from "numerous sensors on the device." (*National Security Agency*) While the NSA and Harris' caution seems grounded in real concerns, I have a hard time imagining most users turning Bluetooth off on their device frequently. Harris might not use AirPods, but I certainly do, and I can vouch anecdotally for the same among many of my friends and family. As in the case of device-based contact tracing, walking around with a phone and sensors and connections enabled is default behavior. Not having a device, or turning off wireless protocols like Bluetooth, is practically aberrant behavior in the eyes of many connected consumers.

Apple's digital Siri assistant is a particularly visible agent of information exchange, one that functions by necessity through always-online, always-listening

hardware devices. After a privacy scandal concerning human review of requests sent to data centers in 2019, the latest version of iOS translates spoken commands into text using hardware acceleration built into each iPhone — though the processing of many requests is still often done on remote servers, even for functionality as simple as "dictating a message." (Bell, *Engadget*) Siri goes beyond a convenience Apple offers its users; it builds a normalized relationship where users willingly talk to and teach a digital personality through their requests and regular patterns. Spellings of words, common habits, and convenient shortcuts are automated through regular use of Siri and artificial intelligence in iOS. Even if learning and processing is done on-device, the nature of Apple's integrated product stack means switching to an Android phone or using non-Apple services would render the training users went through to make their phone smarter useless. The value is moot outside of Apple's control because the information containers are embedded and non-migratable. Although some of this data is synchronized in iCloud for use across Apple devices, leaving the ecosystem presents more challenges still. Siri is perhaps the most prominent example of Apple using artificial intelligence and user data together to create its own beneficial "network effect", constructing a moat of invaluable collected data which it can leverage to its advantage against any other firm that would hope to compete with it. As Gregory et al. at define in a paper on artificial intelligence, "the more that people use it, the more valuable it becomes to each user." (Gregory et al., 1)

Apple's Photo app could easily be mistaken for a basic operating system utility, like File Explorer in Windows or a web browser like Safari. While the app is a basic

place to see pictures taken with the iPhone camera, it also contains myriad intelligent features making use of Apple's machine learning and on-device processing capital. These features of course, rely on a library of photos presumably belonging to the user of the device. Apple is using its smarts to serve users a curated catalog of photos, with a "focus on their best shots" (Apple, Photos Tech Brief, 6) as ranked by an undisclosed algorithm and model. While photos are stored in standard JPEG or HEIF containers commonly used across the tech industry, the metadata and intelligent indexing done by Apple is all proprietary —if you've wondered why your phone heats up the first few days of setup, it's because the device is processing your entire photo library and scanning it to index scenes, people, pets, etc. Aside from this physical evidence of warm iPhones upon setup, Apple's iOS software gives me no indications that background processes are going on. Apple's brief on its Photos app explains this process, but to the average user, the indexing is intended to be seamless. This data is described as a "private, on-device knowledge graph," (8) but aside from seeing it work when searching for photos I have no way as a user see any representation or portable format for this knowledge. It simply lives somewhere mysterious, deeply embedded in my iPhone's hardware. Notably, I can manually tag people in photos and that data will be synchronized off my device, but the mechanics and format of this data are also proprietary and invisible, occurring somewhere in the stack of technology underpinning iCloud photo syncing.

Drawing on the prior mentioned Gregor et al. research, the "scale of the network" (545) in this case is the considerable size of a personal photo library, easily

numbering in the thousands of images accrued over years of using an iPhone. The applications of this technology to “real-time image recognition, face detection, text prediction, and speaker identification” (Gregory et al, 546) are versatile and add even more fuel to an iDevice’s broad swath of user data. The latest iterations of Apple software also use on-device processing to enable users to select and copy scanned text from their photos, be it street signs or chalkboards full of lecture notes. While technically impressive, the aggressiveness with which Apple hardware and software collects info should give users pause. What are we giving our devices with which we take thousands of photos and recordings? Do we own any of that data and could we move it to a rival platform like OneDrive, Google Photos, or our own local hard drive? While photos are standardized, the suite of data we use to organize and collect them is largely in the hands of Apple and its powerful ecosystem. Once we come to take it for granted that we can select text and recognize objects from our photos, we take for granted that we keep paying for iCloud and using iphones. From my ethnographic experience on iOS, this data is useful and impressive but also precarious in the dependence on Apple-proprietary technologies.

Conclusions and Discussion

The hegemonic narrative of capitalism suggests that Apple is an extraordinarily competent business whose products benefit from unilateral control and constant integration between each other. A critical political economic view of the firm sees its products as agents of information exchange, full of data externalities that benefit the

company in perhaps unfair ways that should be understood by the public. The justification for such an analysis lies in the value of understanding the products and services we depend upon. Apple should not be taken as a hardware vendor that provides software and services as a 'bonus' to its users, and it should not be ignored while all the focus of Big Tech scrutiny in the public lies on scandal-laden and widely-panned firms like Facebook.

Audience labor theory sees tech users as a Marxian 'proletariat' and "social media as a factory" (Fisher 1120) in which they work. Labor through leisure is not inherently a problem, but I argue through my research that Apple's information relationship to users shows signs of exploitation, where user data is "separated — or alienated — from its producer" (1109) through the obfuscated and integrated design of Apple's products. Users produce value in using Apple devices but can't transfer much of that information easily to competing hardware or to different software ecosystems. Apple is not alone in the tech industry, as Fisher and others have written about social media's own issues with audience exploitation. Communications studies, in my view, has not gone deep enough on tech firms which integrate hardware and software as deftly as Apple. The company no doubt benefits from its own users' labor in an unequal fashion as the centralized distributor and operator or its devices; its argument is that the gains are mutual, and its users get good products that are private *enough*. Services like Siri and Find My benefit from more users sharing their location, and the Apple Watch's product value lies in leveraging quantifiable health data from people. Social media is a huge agent of the information economy and capitalism, but it isn't

without company. Further up the stack are devices and operating systems people use to access social media and record valuable health data they use in life outside of Facebook. For all the importance of the other Big Tech companies, it seems Apple is uniquely embedded in the real world through its ubiquitous device network.

To keep its hardware profitable and to keep users coming back, Apple software employs artificial intelligence, network effects, and maximizes convenience with tracking features like Find My. All the while, Apple devices hold treasured user data in proprietary formats undisclosed to users. Apple may not be incentivized to sell ads like Google, but it is happy to encourage personal use of its devices and data collection — forming a bond between users and Apple hardware and software. It is certainly possible to migrate digital data off Apple devices, but between features like Find My and the increasing ubiquity of machine learning and Siri in iOS, Apple keeps its ecosystem quarantined from easy exit.

Products like Apple Watch track work, play, and sleep seamlessly and yet they bear uncomfortable relationships to the exploitative healthcare industry in their mass quantification of users. Apple's overall Health initiative is an opportunity for that proprietary Apple ecosystem to meld even more seamlessly into the real, biological world. The consequences of this expansion make the triviality of switching phones take on new weight — imagine the future where healthcare, employment, and your loved ones' data is also embedded in your choice of platform. That world is at our doorstep, delivered by UPS; it's the iPhone in your pocket and the Apple Watch on your wrist.

Bibliography:

Albertgotti, Reed, and Drew Harwell. “Apple and Google Are Building a Virus-Tracking System. Health Officials Say It Will Be Practically Useless.” *Washington Post*, 5 May 2020. *www.washingtonpost.com*, https://www.washingtonpost.com/technology/2020/05/15/app-apple-google-virus/.

Apple. “Apple Advances Its Privacy Leadership with IOS 15, IPadOS 15, MacOS Monterey, and WatchOS 8.” *Apple Newsroom*, 7 June 2021, https://www.apple.com/newsroom/2021/06/apple-advances-its-privacy-leadership-with-ios-15-ipados-15-macos-monterey-and-watchos-8/.

Apple. *Photos Tech Brief*. Sept. 2019, https://www.apple.com/ios/photos/pdf/Photos_Tech_Brief_Sept_2019.pdf. Apple Privacy.

“Apple Reports Fourth Quarter Results.” *Apple Newsroom*, 28 Oct. 2021, https://www.apple.com/newsroom/2021/10/apple-reports-fourth-quarter-results/.

“Apple and Google Partner on COVID-19 Contact Tracing Technology.” Apple Newsroom, 10 Apr. 2021, https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/.

“Attain by Aetna-Fb.” *Aetna*, https://www.attainbyaetna.com/index.html. Accessed 8 Dec. 2021.

Eran, Fisher. “Class Struggles in the Digital Frontier: Audience Labour Theory and Social Media Users.” Information, Communication, & Society, vol. 18, no. 9, 2015.

Limiting Location Data Exposure. National Security Agency, Aug. 2020. Cybersecurity Information.

Rawnsley, Scott Bixby, Shannon Vavra,Adam. “Actually, Kamala Is Right. Bluetooth Is a Risk.” The Daily Beast, 7 Dec. 2021. www.thedailybeast.com, https://www.thedailybeast.com/well-actually-vice-president-kamala-harris-is-right-bluetooth-is-a-risk.

Bell, Karissa. “Apple Moves Siri’s Speech Recognition Offline with New Privacy Updates.” *Engadget*, 7 June 2021, https://www.engadget.com/ios-15-siri-on-device-app-privacy-181525551.html.

Evans, Jonny. “Apple Watch, Health Insurance and the Future of Work.” *Computerworld*, 1 Dec. 2015, https://www.computerworld.com/article/3010527/apple-watch-health-insurance-and-the-future-of-work.html.

Gurdus, Lizzy. “Tim Cook: Apple’s Greatest Contribution Will Be ‘about Health.’” *CNBC*, 8 Jan. 2019, https://www.cnbc.com/2019/01/08/tim-cook-teases-new-apple-services-tied-to-health-care.html.

Liedtke, Michael and AP Business Writers. “Lawmakers Batter Big Tech CEOs, but Don’t Land Many Blows.” *ABC News*, 29 July 2020, https://abcnews.go.com/Business/wireStory/big-tech-ceos-heat-congress-competition-72048090.

Perez, Sarah. “Tile Bashes Apple’s New AirTag as Unfair Competition.” *TechCrunch*, 20 Apr. 2021, https://social.techcrunch.com/2021/04/20/tile-bashes-apples-new-airtag-as-unfair-competition/.

Rich, Jessica. “How Our Outdated Privacy Laws Doomed Contact-Tracing Apps.” *Brookings*, 28 Jan. 2021, https://www.brookings.edu/blog/techtank/2021/01/28/how-our-outdated-privacy-laws-doomed-contact-tracing-apps/.

Simon, Michael. “Apple’s IPhone Privacy Billboard Is a Clever CES Troll, but It’s Also Inaccurate.” *Macworld*, 6 Jan. 2019, https://www.macworld.com/article/232305/apple-privacy-billboard.html.

“Apple Platform Security.” *Apple Support*, Apple, May 2021, https://support.apple.com/guide/security/welcome/web.

White, Jeffrey. “Lopez v. Apple, Inc., 5:19-Cv-04577 (N.D.Cal.).” *Docket Alarm*, 10 Feb. 2021, https://www.docketalarm.com/cases/California_Northern_District_Court/5--19-cv-04577/Lopez_v._Apple_Inc/.

Heinrich Alexander, et al. "Who Can Find My Devices? Security and Privacy of Apple's Crowd-Sourced Bluetooth Location Tracking System." Proceedings On Privacy Enhancing Technologies, vol. 2021, no. 3, 1 Jul. 2021, pp. 227 - 245.

Lanius, Candice L.. "Rhetorical Implications of Contact Tracing Mobile Applications: An Examination of Big Data's Work On the Body." Poroi: An Interdisciplinary Journal of Rhetorical Analysis & Invention, vol. 16, no. 1, 1 Jan. 2021, pp. 1 - 19.

Gregory, Robert Wayne, et al. "The Role of Artificial Intelligence and Data Network Effects for Creating User Value." Academy of Management Review, vol. 46, no. 3, 1 Jul. 2021, pp. 534 - 551.

Wilmott, Clancy, et al. "'I Am He. I Am He. Siri Rules': Work and Play with the AppleWatch." European Journal of Cultural Studies, vol. 21, no. 1, 1 Feb. 2018, pp. 78 - 95.

Arnow, Grant. "APPLE WATCH-ING YOU: WHY WEARABLE TECHNOLOGY SHOULD BE FEDERALLY REGULATED." Loyola of Los Angeles Law Review, vol. 49, no. 3, 1 Jan. 2017, pp. 607 - 633.