Accept. Accept! Accept!? The Problems, Solutions, and Implications of Digital Privacy

Link to multimodal research paper: https://yesnoperhaps.weebly.com/essay-on-digital-privacy

By: Michele Makhlouf Cavero

Abstract

Digital privacy is an oxymoron. As technology has developed, norms governing the digital world have failed to keep pace and information which we were once able to keep to ourselves is now public. The lack of norms has produced a chaotic environment, in which users hand-over their data in exchange for 'free' access. The only model widely implemented across the industry, the Notice and Choice model, fails to cope with the competing interests of user privacy and business profits. Moreover, it's not clear users are acting rationally, as they could be subject to behavioral biases and a lack of information when relinquishing their data. Through an economic lens, while it could be argued that privacy is simply a higher quality good, some contend digital privacy is a modern market failure; they see privacy as a public good and people's trust in tech companies as a common access resource subject to exploitation. While most scholars agree that there are evident issues, few coincide on how to solve these. Informed consent, however, is widely regarded as vital in designing a functional system. The rise of Big-Data and the threats of data leaks magnify the potential ramifications, so ensuring people are educated to not only consent but do so in an informed manner is a key step forward. On top of this, fostering transparency and establishing value optimal norms that take into account all parties involved may constitute a good starting point towards solving the problem.

Keywords

Digital privacy, Notice and Choice, Privacy Paradox, Big-Data, Data Leaks, Informed Consent, Big-Tech, Regulation, GDPR, CCPA, Market Failure, Education, Transparency

The Current Picture: Digital Privacy as Notice and Choice

The internet's impact on society has been immeasurable. Search engines, social networks, and the infinite amount of information these contain have transformed how we receive and process data. Our Facebook friend list, our Google search history, our Amazon purchases, and the reviews we've left on all of these platforms... they all come down to data. Data grows. Today, there's data for every person — for every purpose. Data that's power. Paradoxically, this bits explosion has left most people powerless, as the digital age has stripped most people of their privacy.

For renowned computer scientist Andreas Weigend, privacy is dead. To Weigend, "the time has come to recognize that privacy is now only an illusion" (Weigend 47). He might be right. The current model used by most websites to obtain their users' consent to collect their information — the Notice and Choice model — is not built around protecting user privacy. Instead, it serves as a capitalistic market-place in which users relinquish their information in exchange for a service. As the name suggests, the Notice and Choice model involves notifying users about the website's privacy policies and allowing the users to decide whether they engage with the site or not (Athey et al. 1). Theoretically, it makes perfect sense; in practice, it fails — miserably.

In an article published under the law firm Cozen O'Connor, Harvard law school graduate Brian Kint explains how the Notice and Choice model is more of a Take it or Leave it: "When faced with the choice

of access or no access, users will choose access, no matter how draconian an organization's information sharing practices may be" (Kint). Kint believes that under the current model, users consistently give up their data regardless of how it's handled by the recipient; whether it's handled in a "draconian" manner or not is irrelevant to users making the choice, as they have no choice in the first place. Why don't users have a choice? Chicago-Kent College of Law professor Richard Warner and University of Illinois computer science professor Robert Sloan explain that consent is limited to passive acquiescence because digital privacy choices are highly constrained (Sloan and Warner 21). The scholars analyze the hypothetical case of Vicky, a woman who wants to buy an ebook and considers Amazon to do so. They explain that while Vicky is free to choose another online seller like Barnes and Noble, "Barnes and Noble's practices are very similar to Amazon's" (21 – 22). As such, if she's to buy the ebook, she either has the choice to *take* Amazon's policy as good, or *leave* it all together and refrain from the transaction. Put more simply: there's no choice if all options are the same.

Susan Athey, professor of economics at Stanford University, along with her colleagues Christian Catalini and Catherine Tucker (MIT professors in technological innovation and management, respectively), explored how the Notice and Choice model falls short in regards to the complexity of human behavior. Their research paper, "The Digital Privacy Paradox: Small Money, Small Costs, Small Talk," studies the results of MIT's digital currency experiment, in which undergraduate students were asked about their privacy concerns and given $100 worth of Bitcoin. By asking the students to rank the importance of different privacy aspects when enrolling, and comparing these to their actual privacy decisions in handling their bitcoin, the researchers studied how their stated preferences can differ from their concrete choices.

Specifically, professor Athey and her colleagues identified that small incentives can have a substantial effect on the choices of an individual, finding empirical evidence of the privacy paradox: the phenomenon that "whereas people say they care about privacy, they are willing to relinquish private data quite easily when incentivized to do so" (Athey et al. 2). Concretely, consider an individual who says he values privacy, but to gain access to a service — the incentive — hands of his personal information. The privacy paradox explains this disconnect, and the Notice and Choice model effectively does not address it. Couple this with the researchers' second finding — that small navigation costs are significant influencers of privacy choices, as users' desire for quick information makes them prone to ignore privacy policies — and it's clear why the Notice and Choice model fails as a framework for a healthy digital ecosystem. It appears the users' propensity for immediate gratification makes them overlook any privacy notice in the first place. The third factor the researchers identified adds to this critique, as they found that users exposed to "irrelevant but reassuring information" were more likely to decrease their digital privacy controls (14 – 15). Specifically, 50% of the students were given additional information on PGP encryption software, which, while thoroughly used in cybersecurity, did not add an extra layer of protection to their cryptocurrency transactions. However, far from becoming more aware of digital tracking and its threats, users that saw additional information about PGP felt reassured and relaxed their privacy choices (17). This finding fits 'perfectly' with the Notice and Choice model, as a false sense of protection can be instilled in the users through these ubiquitous notices.

While Athey and her colleagues specifically explore why the model is too shallow to cope with the complexities of human behavior, other sources point out how Big-Tech is not interested in solving the

problem. In their book *Blown to Bits*, Hal Abelson, Harry Lewis, and Ken Ledeen claim that "corporations, and other authorities are taking advantage of the chaos" (Abelson et al. 4). Today, it's clear Facebook, Google, and Twitter, amongst many others, are profiting from their users' information; interestingly, they're finding it difficult to have a consistent policy — an advantage when you look at the problem. The fact that there has not been a single regulatory entity capable of keeping up with the fast-paced tech industry has allowed for a sort of wild-west, where different corporations have different privacy policies, altogether fueling confusion in people, and, subsequently, their own profits.

In his Ted Talk titled "What if Our Data Could Be Protected Online?", UPS logistics expert Derek Banta explains that the root of the problem lies in the fact that there is not one organization whose sole objective is to protect user privacy. For Banta, businesses are "trying to ride two horses" when they "do things to protect your privacy but at the same time have a data monetization strategy built right into their privacy model" (Banta 3:58 – 4:24) Banta hits the nail on the head when claiming that for-profit businesses face the choice of more profits or more privacy for its users; as their name implies, for-profit businesses' nature is to maximize the former.

With the system broken, Big-Data companies are intensively data-mining their users. In the article titled "The WIRED Guide to Your Personal Data (and Who Is Using It)," journalist Louise Matsakis comprehensively goes over the extent to which Big-Data companies are harvesting user data. As expected, "social media posts, location data, and search-engine queries" are all getting mined through digital tools, like cookies, pixels, and tags. However, it can get a lot more invasive, given some companies may track how people interact with their websites or apps: where they click, tap, zoom... (Matsakis). Major implications arise from this level of tracking, as individuals using these apps may be unaware they're being tracked in the first place. Moreover, while this information might seem benign, it slowly builds up. In their book *Born Digital*, Harvard law school professors John Palfrey and Urs Gasser go over what this level of tracking entails for Digital Natives — people born after 1980 who've grown up surrounded by technology. They explain that "by the time a Digital Native enters the workforce there are hundreds — if not thousands — of digital files about her, held in different hands, each including a series of data points that relate to her and her activities" (Gasser and Palfrey 54). The amount of bits, and the fact that these are scattered, makes it illogical to think that a Digital Native can "know that each of these files exist", much less "manage," or "sort" them (54). What raises more concern is the fact that Digital Natives can't often make amends to their information, "even when it turned out to be inaccurate" (54). George Washington University Law School professor Daniel Solove sums this up by claiming that if we continue with our current practices "we will be forced to live with a detailed record beginning with childhood that will stay with us for life wherever we go, searchable and accessible from anywhere in the world" (Solove 17). Under the current model, our digital footprints are set to follow us — and due to our advanced data collection capabilities, these footprints won't wash away. What's more, it's not just that there are thousands of data points, that these are held by countless unknown third parties, or that there's no way to correct this information, but that this data can get pooled together to reveal political positions, behavioral patterns, and predispositions to disease (Brady 2, 5, 10).

Data Breaches, the Lack of Consent, and the Lack of Informed Consent

Perhaps what's more worrying is that data leaks endanger the information of individuals (Abelson et al. 3). Just in 2018, Quora, Under Armour, Marriott, Google, amongst many others, faced significant data

breaches (Leskin). Most notably, the Cambridge Analytica Data Scandal took place. The far-right wing political consulting group exploited "a loophole in Facebook's API that allowed third-party developers to collect data not only from users of their apps but from all of the people in those users' friends network" (Romano). Specifically, Cambridge Analytica simply surveyed 270,000 Facebook users through a third-party app; in doing so, they not only gathered the information of the 270,000 users who had agreed to the app's privacy terms but also that of their friends... amounting to a data pool of 87 million users (Chang). Cambridge Analytica then analyzed these users' likes, grouping them into different psychological categories, which it then used to launch targeted political advertisements (Hannes Grassegger & Mikael Krogerus).

While evaluating the impact Cambridge Analytica has had on world politics could easily be the subject of an entire research paper (the firm was involved in Trump and Brexit campaigns), the key takeaway from this case study is that neither Notice or Choice was given to most of the 87 million users. For this, Mark Zuckerberg apologized on a CNN interview: "This was a major breach of trust, and I'm really sorry that this happened" (Zuckerberg 00:05 – 00:12). Notice that not notifying users that their data was being shared transgressed Facebook's policy, but it is actually common practice for most in the digital industry.

In fact, in his New York Times article titled "This Article is Spying on You," Carnegie Mellon computer science professor Timothy Libert explains that "only 10 percent of these outside parties [that mine your information] are disclosed in privacy policies of the news sites we studied, meaning even diligent readers will never learn who collects their data" (Libert). In other words, the Notice and Choice model is not applied across digital platforms, and even when it is, it omits critical information about the true scope of data collection.

For the sake of the current model, however, assume that the Notice and Choice model is applied consistently and that it reports 100% of the data-mining third parties. Even if this is the case, and the user consents, the model falls short due to the lack of *informed* consent. As discussed previously, the model fails to provide a framework in which users can become informed participants of the digital community. Zuckerberg himself recognized this in April of 2018 when he testified for the Senate of Commerce and the Senate of Judiciary committees to inform their investigation on "Facebook, Social Media Privacy, and the Use and Abuse of Data." Specifically, when senator Lindsey Graham asked, "do you think the average consumer understands what they're signing up for?", Zuckerberg responded: "I don't think that the average person likely reads that whole document" ("Facebook, Social Media Privacy, and the Use and Abuse of Data" 1:31:08 – 1:31:45). That's partly on the user for not reading the document, but it's also on Facebook for taking their users' consent as good despite knowing it is uninformed. In this regard, perhaps some sort of government intervention is needed to hold firms like Facebook accountable, or at least make the people who accept Facebook's terms fully aware of what that entails for their privacy.

Historically, there are cases in which government intervention was needed to address the lack of informed consent. Take the tobacco industry. In the mid-1960s, more than 40% of the US adult population smoked tobacco ("Overall Tobacco Trends"). However, throughout the 20th century and particularly since the 1950s, medical research had been consistently finding that tobacco smoke is harmful to human health (Proctor 87). The 1964 Surgeon's General report officialized these findings, leading to a series of government regulations aimed at informing smokers of the adverse health effects: by 1966 the Cigarette

and Labelling and Advertising Act of 1965 came into force and required a vague health warning to accompany each pack; by 1970 the Public Health and Cigarette Smoking Act made this labeling stronger; by 1984 the Comprehensive Smoking Education Act required tobacco packages and advertisements to rotate between four affirmative warnings; by 2009 former President Barack Obama signed the Family Smoking and Prevention Tobacco Control Act, which gave the FDA the power to regulate the industry, and led to the current push for graphic warnings (*Centers for Disease Control and Prevention*). All in all, these measures helped reduce smoking from more than 40% in 1965 to 14% in 2017 ("Overall Tobacco Trends"). This is why Penn State behavioral health professor Lynn Kozlowski believes informed consent needs to be taken even further: labels should be more specific "to include information on the degree of risks" (Kozlowski ii3). Similarly, the GDPR, Europe's new legislation on consumer data processing, is based on informed consent. The official legal document specifically explains what constitutes valid consent: "Consent should be given by a clear affirmative act establishing a freely given, specific, *informed* and unambiguous indication of the data subject's agreement to the processing of personal data relating to him" [emphasis added] (*Official Journal of the European Union* L/119/6). In the case of tobacco, it is important to note that for the US government consent proved to be insufficient. It wasn't a matter of consent — of deciding to smoke — but of informed consent — of deciding to smoke knowing about the adverse health consequences. As the GDPR shows, the same argument is valid to support regulation within the digital privacy realm. For a user to truly have digital privacy it's not only about consent — about agreeing to the site's terms — but also about informed consent — about agreeing to the site's terms knowing precisely about the privacy implications.

The Push for Regulation: Warren vs. Big-Tech

Elizabeth Warren is one of the few politicians aware that there is a systematic problem and bold enough to point it out. The rising Democratic candidate for the US 2020 presidential election has made it clear that if she wins, she'll make sure to regulate the Big-Tech industry. In a Medium article titled "Here's how we can break up Big-Tech," Warren explains her plan to break up data-mining giants such as Amazon, Google, and Facebook; according to her, these companies have "too much power — too much power over our economy, our society, and our democracy" (Warren). That's a claim that is hard to challenge. More specifically, Warren gives three reasons to sustain her proposal to break up Big-Tech: Number one, that Big-Tech firms are engaging in anti-competitive behavior; Number two, that Big-Tech firms should not be capable of undermining the USA's electoral security; Number three, that Big-Tech firms are exploiting users' privacy (Warren). Warren has been very active on Twitter advocating for her solution. In fact, to this date (11/17/2019), Warren has tweeted more than 100 times about how splitting the tech giants would improve the industry's practices. By splitting them up, she argues, companies would compete to secure user privacy rather than sell user information (Warren).

This has not gone unnoticed by major Big-Tech players. At an internal Facebook meeting in July — audio from which was leaked to The Verge by one of the employees who assisted — Zuckerberg criticized Elizabeth Warren for thinking that "the right answer is to break-up the companies" (Zuckerberg / The Verge). Zuckerberg justified his position by recognizing that while they "care about [their] country and want to work with [their] government [...] if someone is going to challenge something that existential you go to that mat, and you fight". Major Big-Tech player Bill Gates, who is also the world's most generous philanthropist, agrees with Zuckerberg in that breaking up Big-Tech is not the answer. In an interview with Bloomberg, the Microsoft founder explained why Warren's proposal is overly

simplistic: “If there is a way a company is behaving that you want to get rid of, then you should just say ‘okay that’s a banned behavior.’ Splitting the company in two and having two people doing the bad thing doesn’t seem like a solution” (Gates 00:07 – 00:44). Analyzing Warren’s proposal, it’s evident that she aims at providing a single solution to address many problems — making succeeding much harder. Warren draws distinctions between all the tech mammoths to present the many issues within the industry — Big-Tech firms engaging in anti-competitive behavior, their power to undermine the USA’s electoral security, and foregoing user privacy for greater profits — but then reduces all of these problems to one solution: Breaking-up Big-Tech. For instance, Warren has lumped Apple — a company that does not sell its users’ data — with data selling companies Google, Facebook, and Amazon. It does not add up. What also doesn’t add up is that for some arbitrary reason, the split-up will only target firms with annual revenues of more than $25 billion... but size in itself is not a crime — behavior is. Moreover, many of the behaviors Warren is so blatantly calling out are not specific to the tech industry. Warren’s rationale for splitting Apple is based on their ability to discriminate against third-party developers in favor of their own apps, but, as Tim Cook explained in an interview with CNBC, one would think that if one owns a store one is free to choose what is sold on that store (Cook 15:10 – 15:30). While some might argue that Warren has included Apple not only because of their ability to promote their apps in their Apple Store but also because of their market share and the complex externalities of virtualization, it is an arbitrary addition that seems more focused on other factors such as gaining media coverage.

Indeed, there is a political component to Warren’s proposal. Perhaps sparking this debate has been part of Warren’s strategy to gain voters’ preference. After all, before she can implement anything, she has to win the electoral race. Why has Warren called out Facebook and Amazon much more than Google or Apple? It could be about data collection capabilities or revenue, but there’s also the political-impact factor. The Cambridge Analytica breach deteriorated Facebook’s reputation, and ever since Jeff Bezos became the wealthiest person in the world there’s been certain resentment towards Amazon, especially considering Amazon’s ability to avoid taxes has been well documented by the media — and Warren is capitalizing. On the other hand, it’s also true that because it’s politics and we’re just in the primaries, Warren doesn’t have to be this specific this early on. By drafting her ideas into public proposals, she incurs a massive political risk and exposes herself to criticism. No other candidate is doing this, and Warren’s forthright approach is refreshing. It’s also unfair to judge the contents of a proposal as if it were a finalized bill. Under the current political system, when a proposal is released rarely does it remain unchanged.

Former Secretary of Labor Robert Reich agrees with Warren in that the answer is to split up the companies. In an Inequality Media production, Reich explains that the rapid development of the tech industry has translated into a second Gilded Age: whereas in the late 1800’s steel production and oil extraction fueled huge monopolies, today’s digital advancements enable a similar outcome (Reich). Like Warren, he believes that the tech giants are “stifling innovation,” “undermining our democracy,” “hurting the environment,” and not sharing “their huge wealth with their workers” (Reich). While I personally don’t share their ideologies nor their approach towards solving the issue, both Warren’s and Reich’s push to break up the companies reflect their long-term pursuit against concentrated wealth.

Although the two Democrats raise valid concerns, in reality, Big-Tech firms are not evil. In fact, they’re doing lots of good: Facebook is connecting people in unimaginable ways, Amazon is providing a market-place for entrepreneurs to thrive, Google provides tools that are accessible to all, and Apple has saved

lives by alerting their Apple Watch users if the watch senses signs of Afib, amongst others. While doing some good does not make-up for doing some bad, it's essential to keep in mind that these companies' behavior does not follow a strict dichotomy. It's not as simple as a binary choice in which either all are good or all are evil. In any case, splitting the firms and hoping this will somehow fix the industry seems reckless. On the more positive side, Warren has been successful in getting a nation-wide conversation started, making people aware of the degree of power that these Big-Tech companies have, and at least attempting to address an evident issue.

Digital Privacy as an Economic Problem

In terms of regulating the tech mammoths, California is far ahead of the rest of the United States. After the Cambridge Analytica scandal, the state took steps to protect user privacy, passing the California Consumer Privacy Act of 2018 ("California Consumer Privacy Act"). Similar to the GDPR, the CCPA aims at providing a safe web-surfing environment. To accomplish this, the legislation grants four new laws to Californian users:

1. Awareness: "The right to know what personal information is collected, used, shared or sold."
2. Deletion: "The right to delete personal information held by businesses."
3. Choice: "The right to opt-out of sale of personal information. Consumers are able to direct a business that sells personal information to stop selling that information."
4. Real Choice: "The right to non-discrimination in terms of price or service when a consumer exercises a privacy right under CCPA" ("California Consumer Privacy Act").

By securing these rights, particularly #3 and #4, the CCPA brings real actual choice to what today is the 'Take-it or Leave-it.' Under the CCPA, users will not only have the right to know what information is being tracked and delete it but also completely opt-out of the tracking in the first place — without detriment.

However, in doing so, it could wreck the business model of data-mining companies. Why? Because why would any person want their data to be used and sold if it's not necessary? Perhaps everyone is going to opt-out. That's like going over to store and having the option to either pay or not pay... but either way, you get the product. It's economically unsustainable. Regulators, however, want to take it even further. California Governor Gavin Newsome has proposed the idea of a 'data dividend' aimed at rebalancing the power structure between Big-Tech companies and their users. According to the governor, "California's consumers should also be able to share in the wealth that is created from their data" (Newsome 38:50 — 39:53). Nevertheless, users do reap the benefits of their data: users have access to online services, information, and networks for free — at least in terms of money. Up to now, data has been the way users have been paying for these 'free' services, and all of these regulations simply put the free model at risk. As CEO of Admiral (a consulting company that helps tech companies overcome adblockers) Dan Rua explains, the only reason why most sites are free is "because of advertisements working" (qtd. in Bauer). If Big-Data companies' ability to collect and sell information is restrained, these companies will simply need to find another way to make a profit. As such, there would be a systematic switch to "paid alternatives such as the Freemium model, the Fee-for-service model or the Subscription model," which would, in turn, worsen the digital divide and further inequality (Sanchez and Viejo 114). Simply put, if websites are unable to make money off our information, they might have to start charging for their

services.

As expected, this is something most users don't even want. In the aforementioned study "Small Money, Small Costs, Small Talk," professors Athey, Catalini, and Tucker found that "when expressing a preference for privacy is essentially costless as it is in surveys, consumers are eager to express such a preference, but when faced with small costs this taste for privacy quickly dissipates" (Athey et al. 4). Assistant professor of economics at Grove City College Caleb Fuller examines this dissonance from a purely economic lens and goes even further by claiming that digital privacy paradox may not even exist: "It is possible to explain the so-called "privacy paradox" by showing that individuals express greater demands for digital privacy when they are not forced to consider the opportunity cost of that choice" (Fuller 371). Examined economically, for most people privacy is simply a higher quality good — they see value in it but are not willing to pay for it. Fuller concludes that "consumers prefer exchanging information to exchanging money" (371). Does this signify a market failure? Fuller believes not. The economics professor identifies the three sources where digital privacy market failure could potentially arise — asymmetric information between businesses and users, users' behavioral biases, and data resale externalities — and rejects these. Regarding asymmetric information, Fuller claims that in every complex good market no one is perfectly informed (363). Regarding behavioral biases, Fuller explains that users are not biased but simply reacting to price constraints, as people signal a higher preference for privacy when they do not have to incur a cost (368). Regarding data reselling externalities, meaning negative externalities that users face when unwanted third parties access their data, he explains that as in any other economic trade these are priced in at the moment of the initial transaction (369). He adds compelling evidence to this last argument as he reasons that "if the possibility of information resale imposes a negative externality on a digital user, the logical conclusion seems to be that every mutually beneficial exchange [...] is rife with the possibility of generating negative externalities" (369). In other words, in any transaction the possibility of the supplier using the generated resources to engage in an activity that the "initial consumer dislikes" is present, and that rather than constituting a market failure this is simply a "psychic loss" — a "possibility in every transaction" (369). All in all, Fuller concludes that evidence for market failure is lacking and, as a result, the push for regulation should be reconsidered.

Fuller, however, is too absolute in his analysis. To scrutinize the sources of market failure, the professor conducted a survey in which people had to respond to a series of privacy questions that involved their level of awareness about Google's data collection capabilities and how much they would be willing to pay for their privacy. One of his main findings was that people were generally well informed. However, in making this claim he overlooked the potential implications of an issue he did identify: that "respondents clearly are far less well-informed about *how* Google *uses* their data than that personal information is collected" [emphasis added] (Fuller 10). When he later claims that data reselling externalities are priced in at the moment the transaction is made, that opposes his own finding that individuals are uninformed about *how* their data is *used*. In other words, if users don't know how their data is used, how could they possibly price data reselling externalities the moment they engage in the transaction? Moreover, even if users are well-informed, they might then fall to behavioral biases, as they might irrationally believe that data reselling is not going to affect them specifically. Put more succinctly: immediate gratification bias, which often causes people to disregard future outcomes in preference of an instantaneous benefit. Fuller acknowledges this bias, but claims that "to explain behavior in digital environments [referring to the privacy paradox], appeal to immediate-gratification bias need not be necessary or even helpful. Instead,

consumers simply may be unwilling to bear the cost of obtaining a higher-quality search engine" (368). While this could be true, it might as well be that the combination of all of these and other factors generate the privacy paradox. In fact, Fuller quotes economics professors Alessandro Acquisti (Carnegie Mellon University), Curtis Taylor (Duke), and Liad Wagman (Illinois Institute of Technology) at the start of his paper to present an overarching picture of previous work on the topic, but does not unify their theory with his when concluding. Specifically, Acquisti and his colleagues explain that "the dichotomy between privacy attitudes and privacy behaviors is actually the result of many coexisting, and not mutually exclusive factors" [referring to behavioral biases and asymmetric information] (Acquisti 477). Perhaps it would be relevant to explore the possibility of the privacy paradox arising due to market failure in terms of people's behavioral biases and asymmetric information — as Acquisti, Taylor, and Wagman suggest — but being magnified by the fact that users see privacy as a higher quality good — as Fuller suggests.

More generally, other scholars point at other factors that could induce market failure. Law school professor at Duke university Joshua Fairfield alongside his colleague Cristopher Engel from the University of Bon contend that privacy shares properties of public goods; as such, there is an under allocation of resources towards its preservation (Engel and Fairfield 421). Similarly, research professor Nikolas Laoutaris from IMDEA Networks Institute considers that "consumer privacy and trust in the web [...] are a shared commons that can be overharvested to the point of destruction" (Laoutaris 1868). Moreover, even if market failure does not apply, it is hard to compare personal data to other complex goods, as privacy is considered a fundamental human right ("The Universal Declaration of Human Rights"). The notion of selling a human right is — to say the least — problematic. Nevertheless, Fuller's economic analysis is still a valuable contribution to the conversation as it sheds light on how we should go about solving the issue: it could be all about changing demand... about changing consumer preferences. If we increase the value users put on their privacy, users will start demanding privacy-preserving options and be more willing to pay for these. In doing so, the companies many politicians have blatantly called out for reacting to consumer demand will need to adjust. As such, perhaps we should not start with regulation but with education.

First Education. Then Regulation…?

Major Big-Tech companies' recent policy changes in regards to political advertisement are proof of how consumer preferences can influence how these businesses operate. In October 2019, Twitter's CEO, Jack Dorsey, announced that Twitter would be banning political advertisements (Dorsey). While the policy has been amended to allow for activism, social stewardship, and civic engagement, put simply, Twitter's new policy bans all political advertisements — and they're already enforcing it.

The rationale behind this radical but responsible change lies in their belief that "political message reach should be earned, not bought" ("Political Content"). Less than a month after Twitter's announcement, Google hopped on through an official blog post in which they communicated that starting January 2020 they'll be enforcing new world-wide regulations on political advertisements. While Google will not ban these, they'll be limiting the targeting capabilities of advertisers: psychographically to "contextual targeting" (interests), and demographically to "age, gender, and general location (postal code level)" (Spencer). Moreover, in the same post, Google reiterated its commitment towards debunking Fake News and creating a transparent online ecosystem. While it's true that Facebook has not followed suit, they have explained how they're getting ready for the 2020 US presidential elections. Their strategy

involves increasing transparency through a "seven year library," "cracking down on fake accounts," "bringing in fact-checkers," and "investing heavily in AI to take down harmful content" (Clegg). Indeed, it's true they're still taking advertisement dollars and controversially excepting politicians from their third-party fact-checkers, but they are taking some steps to address the issue. While Twitter, Google, and Facebook are targeting the issue to a lesser or greater extent, they have one thing in common: they're all addressing the problem and letting the public know they're doing so. Why? Because their users are starting to demand so.

These policy changes can be ultimately traced back to Russia's illegal meddling of the 2016 US presidential election. Russian interference involved hacking key people in Clinton's campaign, intruding into voters databases, and most notably using social networks (Facebook, Twitter, and Google+, amongst many others) to discourage African Americans from voting, encouraging conservatives to vote, and creating troll accounts to systematically criticize Hillary Clinton and support Donald Trump (Madrigal). All in all, the overall strategy was to harm the likes of the democratic candidate from winning the presidential race, as Russian President Vladimir Putin thought Clinton's electoral win would be detrimental to Russia ("Intelligence Report on Russian Hacking" 7). The scandal came to light in September 2016 and led to an FBI investigation that Trump unsuccessfully attempted to dismantle by terminating FBI director James Comey (Law and Bogholtz). After Comey's discharge, Democrats pushed for Special Counsel investigation, which they ended up getting: Former FBI agent Robert Mueller continued the work of Comey, conducting a two-year investigation (Mueller 89). In April of 2019, the report was published with an ambivalent conclusion that reached no final verdict: "while this report does not conclude that the President committed a crime, it also does not exonerate him" (Barr 2). Despite this anticlimactic outcome, the scandal captured the national conversation for more than two years, and by the end of the investigation the public was aware of the vulnerabilities of the USA's electoral system and the role that social networks could potentially play on an election. Social media networks were called out both by the media and the general public. Since then many of the involved tech businesses have publicly apologized or recognized their mistakes: Tumblr has published a "public record of usernames linked to state sponsored disinformation campaigns" ("Public Record of Usernames"), Twitter's former CEO and co-founder Evan Williams apologized "for making Trump's presidency possible" while on Twitter's board (Williams), and Mark Zuckerberg apologized before Congress ("Facebook, Social Media Privacy, and the Use and Abuse of Data" 39:50 – 40:50). Without public pressure and intense media coverage, these firms would have probably avoided recognizing their mistakes. Linking back to the economic discussion, without the rise of informed users challenging the companies' practices, these companies would have avoided losing political advertisement dollars. As such, educating users proves vital in ensuring a functional system.

But just education will probably be insufficient. Recall the comparison made about how tobacco regulation throughout the 20th century sheds light on why regulation is appropriate in the digital privacy realm. Regulation was used to ensure not only consent but also informed consent. Going back to the case study, in 1966 when health warning labels were first proposed, "multinational tobacco companies did not object to voluntary innocuous warnings with ambiguous health messages," and only after regulators pushed to make the labels affirmative did the industry start lobbying against these (Hiilamo et al. 1). Analogically, the Notice and Choice model provides these *innocuous* and *ambiguous* warnings all of the Big-Tech firms have readily embraced, and only after regulators started pushing for a more transparent

system have Big-Tech firms started lobbying against these. This comparison gains relevance when analyzing why tobacco companies then and Big-Tech firms now do not oppose these vague messages: legal liability (Hiilamo et al. 1; Kint). Despite the different industry and time-period, the motive behind their modus-operandi is the same: tobacco companies then and Big-Tech firms now do not oppose vague messages to protect themselves from legal liability, yet do oppose stronger regulation to continue profiting from their users' lack of informed consent. Through this lens, regulation is necessary to make for-profit businesses protect both their profits and their users. The solution, therefore, involves not only educating or regulating but both: it's about guaranteeing education through regulation.

Stakeholders' Responsibilities

Is guaranteeing education through regulation going to be enough? Probably not — but it is a start. For education to have a significant impact, there need to be ways for people to exercise this new education. Previously cited to explain why user consent is limited to passive acquiescence, professors Warner and Sloan call to question the lack of norms in the digital environment. As they reason, "rapid advancements in technology have outstripped the relatively slow evolution of norms and created novel situations for which we lack relevant value optimal norms" (Sloan and Warner 29). These value optimal norms refer to a set of rules that regulate data collection, such that no other alternative generates a better trade-off in terms of both the interest of users and businesses. In this sense, the government should work as a facilitator of this optimality. The GDPR and the CCPA are valid attempts at creating an environment in which these optimal trade-offs can occur, but there are still unaccounted externalities that need to be investigated for a truly optimal market outcome to rise. For this to happen, the government and advocacy groups, together with industry leaders, should strive to define solutions that work for every stakeholder.

However, many issues challenge a market outcome in which all stakeholders can thrive. First, the fact that governments can act as fair umpires is dubious at best. Officers will need to work to protect user privacy without undermining the tech industry, all while keeping their own interests at bay. Lobbies and the pursuit of notoriety are significant influencers of individual politicians, and national security interests directly oppose those of digital privacy. For instance, on October of 2019, the USA, the UK, and Australia publicly exerted pressure on Facebook to stop expanding their end-to-end encryption services, which would grant its users with increased privacy (Lomas). As such, it's sensible to question with which motive will governments intervene. Will they prioritize the privacy of their citizens, or will they prioritize their surveillance capabilities? Going back to logistics expert Derek Banta's discussion on trying to ride two horses at once, for an optimum market outcome to occur governments will need to choose only one. Hopefully, they'll choose the right one.

However, it's hardly *only* the government's responsibility to protect people's privacy. Firms need to internalize that they face a moral duty to protect their users' information and that this could sometimes come at the expense of their profits. While some might reasonably challenge for-profit businesses' ability to refrain from infringing informational norms, this is the main reason firms should be part of the process when creating these. Moreover, there's also the question of how to educate users efficiently so as to maximize market outcomes. Of course, it's unreasonable to think that everyone will be able to grasp the complexities of the digital ecosystem fully. In this respect, Warner and Sloan argue that informational norms can help overcome this issue, as with the norms at place less specific details — and, consequently, less education — will be necessary for informed consent to hold (Sloan and Warner 31).

For the involved parties to collaborate effectively, transparency is key. Governments need to be straightforward about their intentions, and the tech companies should be held to the same standards and be sincere about their practices. Professor Laoutaris highlights the importance of transparency as he claims it's "the guiding light pointing to problematic technologies and business practices" (Laoutaris 1868). He then extrapolates this argument to contend that because "complex technology can only be tamed by other, equally advanced, technology [...] online data protection needs to develop its transparency methods and software" (1869). In other words, Laoutaris believes that empowering users with programs for them to verify the industry's practices is necessary to address the current privacy problems — calling for the rapid development of these tools. This would open the market to new opportunities, which would, in turn, address Warren's and Reich's concern about the decreasing number of tech start-ups. As such, while the intricacies of the digital world make it hard to pinpoint the problem, perhaps it's not impossible to find a solution that works for all.

Acknowledgements
I want to thank professor Ryan Sloan for his continuous guidance throughout the project; his encouragement throughout the research, feedback on the drafts, and push-back on my personal biases ultimately led me to write a more comprehensive and critical paper.

Works Cited

Abelson, Harold, et al. *Blown to Bits: Your Life, Liberty, and Happiness after the Digital Explosion*. Addison-Wesley, 2018.

Abrams, Abigail. "Here's What We Know So Far About Russia's 2016 Meddling." *Time*, Time, 18 Apr. 2019, time.com/5565991/russia-influence-2016-election/.

Acquisti, Alessandro, et al. "The Economics of Privacy." *Journal of Economic Literature*, vol. 54, no. 2, 2016, pp. 442–492., doi:10.1257/jel.54.2.442.

Armerding, Taylor. "The 18 Biggest Data Breaches of the 21st Century." *CSO Online*, CSO, 20 Dec. 2018, www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.

Athey, Susan, et al. "The Digital Privacy Paradox: Small Money, Small Costs, Small Talk." *National Bureau of Economic Research*, 2017, doi:10.3386/w23488.

Bae, Michelle, and Gabriela Zanfir-Fortuna. "CCPA, Face to Face with the GDPR: An in Depth Comparative Analysis." *Future of Privacy Forum ICal*, 28 Nov. 2018, fpf.org/2018/11/28/fpf-and-dataguidance-comparison-guide-gdpr-vs-ccpa/.

Banta, Derek, speaker. *What If Our Data Could Be Protected Online? TED*, www.ted.com/talks/derek_banta_what_if_our_data_could_be_protected_online/up-next.

Barr, William P. "Read Attorney General William Barr's Summary of the Mueller Report." *The New York Times*, The New York Times, 24 Mar. 2019, www.nytimes.com/interactive/2019/03/24/us/politics/barr-letter-mueller-report.html.

Bauer, Meredith Rutland. "Are Ad-Blockers Saving Internet Users, or Ruining the Internet?" *Vice*, 13 Jan. 2017, www.vice.com/en_us/article/vv7nvm/are-ad-blockers-saving-internet-users-or-ruining-the-internet.

Becker, Marcel. "Privacy in the Digital Age: Comparing and Contrasting Individual versus Social Approaches towards Privacy." *Ethics and Information Technology*, vol. 21, no. 4, 2019, pp. 307–317., doi:10.1007/s10676-019-09508-z.

Brady, Henry E. "The Challenge of Big Data and Data Science." *Annual Review of Political Science*, vol. 22, no. 1, 2019, pp. 297–323., doi:10.1146/annurev-polisci-090216-023229.

Burgess, Matt. "What Is GDPR? The Summary Guide to GDPR Compliance in the UK." *WIRED*, WIRED UK, 14 Feb. 2019, www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018.

"California Consumers Express Concerns About the California Consumer Privacy Act: Regulatory Rumblings: Blogs." *Association of National Advertisers: Driving Growth*, 5 Feb. 2019, www.ana.net/blogs/show/id/rr-blog-2019-01-California-Consumers-Express-Concerns-About-The-California-Consumer-Privacy-Act+.

Centers for Disease Control and Prevention, CDC, 13 Dec. 2017, www.cdc.gov/tobacco/data_statistics/by_topic/policy/legislation/index.htm.

Chang, Alvin. "The Facebook and Cambridge Analytica Scandal, Explained with a Simple Diagram." *Vox*, Vox, 2 May 2018, www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram.

Clegg, Nick. "Facebook, Elections and Political Speech." *About Facebook*, 24 Sept. 2019, about.fb.com/news/2019/09/elections-and-political-speech/.

"Consent." *General Data Protection Regulation (GDPR)*, Intersoft Consulting, gdpr-info.eu/issues/consent/.

Cook, Tim. “Watch CNBC’s Full Interview with Apple CEO Tim Cook.” *CNBC*, 6 May 2019, www.cnbc.com/video/2019/05/06/watch-cnbcs-full-interview-with-apple-ceo-tim-cook.html.

Dorsey, Jack. @Jack. “We’ve made the decision to stop all political advertising on Twitter globally. We believe political message reach should be earned, not bought. Why? A few reasons…” *Twitter*, 30 Oct. 2019, https://twitter.com/jack/status/1189634360472829952

“Facebook, Social Media Privacy, and the Use and Abuse of Data.” *Senate Judiciary Committee*, Senate Judiciary Committee and Senate Commerce Committee, Apr. 2018, www.facebook.com/senjudiciary/videos/626181511053468.

Fairfield, Joshua, and Christoph Engel. “Privacy as a Public Good.” *Duke Law Journal*, vol. 65, no. 3, Dec. 2015, pp. 385–457., scholarship.law.duke.edu/cgi/viewcontent.cgi?article=3824&context=dlj.

Feiner, Lauren. “California's New Privacy Law Could Cost Companies a Total of $55 Billion to Get in Compliance.” *CNBC*, CNBC, 8 Oct. 2019, www.cnbc.com/2019/10/05/california-consumer-privacy-act-ccpa-could-cost-companies-55-billion.html.

Fielding, Jon. “Four Differences between the GDPR and the CCPA.” *Help Net Security*, 3 Feb. 2019, www.helpnetsecurity.com/2019/02/04/gdpr-ccpa-differences/.

Friel, Alan, and Laura Jehl. “CCPA and GDPR Comparison Chart.” *Practical Law*, www.bakerlaw.com/webfiles/Privacy/2018/Articles/CCPA-GDPR-Chart.pdf.

Fuller, Caleb S. “Is the Market for Digital Privacy a Failure?” *Public Choice*, vol. 180, no. 3-4, 2019, pp. 353–381., doi:10.1007/s11127-019-00642-2.

Gates, Bill. “Bill Gates Says Big Tech Companies Shouldn’t Be Broken Up.” *Bloomberg Technology*, YouTube, 17 Sept. 2017, www.youtube.com/watch?v=-9xnWNeKpz8.

“GDPR - 8 Rights under GDPR.” *Vivid Fish - UK Inbound Marketing Agency*, 1 Nov. 2017, www.vividfish.co.uk/blog/gdpr-8-rights-under-gdpr.

Gilbert, Ben. “The #DeleteFacebook Movement Has Reached a Fever Pitch, as Former Facebook Insiders Turn on the Company.” *Business Insider*, Business Insider, 21 Mar. 2018, www.businessinsider.com/deletefacebook-facebook-movement-2018-3.

Grassegger, Hannes, and Mikael Krogerus. “The Data That Turned the World Upside Down.” *Vice*, 28 Jan. 2017, www.vice.com/en_us/article/mg9vvn/how-our-likes-helped-trump-win.

Hiilamo, Heikki, et al. “The Evolution of Health Warning Labels on Cigarette Packs: the Role of Precedents, and Tobacco Industry Strategies to Block Diffusion.” *Tobacco Control*, vol. 23, no. 1, 2012, doi:10.1136/tobaccocontrol-2012-050541.

“Intelligence Report on Russian Hacking.” *The New York Times*, The New York Times, 6 Jan. 2017, www.nytimes.com/interactive/2017/01/06/us/politics/document-russia-hacking-report-intelligence-agencies.html.

Kerry, Cameron F., and John B. Morris. “Why Data Ownership Is the Wrong Approach to Protecting Privacy.” *Brookings*, Brookings, 26 June 2019, www.brookings.edu/blog/techtank/2019/06/26/why-data-ownership-is-the-wrong-approach-to-protecting-privacy/.

Kharpal, Arjun. “Everything You Need to Know about a New EU Data Law That Could Shake up Big US Tech.” *CNBC*, CNBC, 25 May 2018, www.cnbc.com/2018/03/30/gdpr-everything-you-need-to-know.html.

Kint, Brian. “Is It Time To Rethink Notice And Choice As A Fair Information Privacy Practice?” *JD Supra*, 14 Feb. 2019, www.jdsupra.com/legalnews/is-it-time-to-rethink-notice-and-choice-95601/.

Kozlowski, L T. “‘Not Safe’ Is Not Enough: Smokers Have a Right to Know More than There Is No Safe Tobacco Product.” *Tobacco Control*, vol. 14, no. suppl II, 2005, pp. ii3–ii7., doi:10.1136/tc.2004.008334.

Krasnow, Melissa J. “A Summary of the California Consumer Privacy Act of 2018.” *A Summary of the California Consumer Privacy Act of 2018 | Expert Commentary | IRMI.com*, Sept. 2018, www.irmi.com/articles/expert-commentary/a-summary-of-ccpa-of-2018.

Kulik, Tom. “Some Big Reasons Why The CCPA Is More Of A Problem Than You Think.” *Above the Law*, Above the Law, 28 Oct. 2019, abovethelaw.com/2019/10/some-big-reasons-why-the-ccpa-is-more-of-a-problem-than-you-think/?rf=1.

Laoutaris, Nikolaos. “Data Transparency: Concerns and Prospects [Point of View].” *Proceedings of the IEEE*, vol. 106, no. 11, 2018, pp. 1867–1871., doi:10.1109/jproc.2018.2872313.

Law, Tara, and Lauren Bogholtz. “Here Are the Biggest Takeaways From the Mueller Report.” *Time*, Time, 22 Apr. 2019, time.com/5567077/mueller-report-release/.

Leskin, Paige. “The 21 Scariest Data Breaches of 2018.” *Business Insider*, Business Insider, 30 Dec. 2018, www.businessinsider.com/data-hacks-breaches-biggest-of-2018-2018-12.

LeVine, Steve. “U.S. Startups Are in a Surprising 13-Year Slump.” *Axios*, 27 May 2018, www.axios.com/startups-slump-13-years-artificial-intelligence-us-ef914164-78f7-4783-b912-2ea50a06968d.html.

Libert, Timothy. “This Article Is Spying on You.” *The New York Times*, The New York Times, 18 Sept. 2019, www.nytimes.com/2019/09/18/opinion/data-privacy-tracking.html.

Lomas, Natasha. “Facebook Is Being Leaned on by US, UK, Australia to Ditch Its End-to-End Encryption Expansion Plan.” *TechCrunch*, TechCrunch, 3 Oct. 2019, techcrunch.com/2019/10/03/facebook-is-being-leant-on-by-us-uk-australia-to-ditch-its-end-to-end-encryption-expansion-plan/.

Madrigal, Alexis C. “What Facebook Did to American Democracy.” *The Atlantic*, Atlantic Media Company, 16 Nov. 2017, www.theatlantic.com/technology/archive/2017/10/what-facebook-did/542502/.

Matsakis, Louise. “The WIRED Guide to Your Personal Data (and Who Is Using It).” *Wired*, Conde Nast, 19 Feb. 2019, www.wired.com/story/wired-guide-personal-data-collection/.

Meixler, Eli. “Mark Zuckerberg Apologizes For Facebook Data Scandal.” *Time*, Time, 22 Mar. 2018, time.com/5210191/mark-zuckerberg-cnn-facebook-cambridge-analytica-data/.

“The Mueller Report, Annotated.” *The Washington Post*, WP Company, 18 Apr. 2019, www.washingtonpost.com/graphics/2019/politics/read-the-mueller-report/.

Mueller, Robert. *Report On The Investigation Into Russian Interference In The 2016 Presidential Election Volume I of II*. U.S. Department of Justice, 2019, *Report On The Investigation Into Russian Interference In The 2016 Presidential Election Volume I of II*, https://www.justice.gov/storage/report.pdf

Mueller, Robert. *Report On The Investigation Into Russian Interference In The 2016 Presidential Election Volume II of II*. U.S. Department of Justice, 2019, *Report On The Investigation Into Russian Interference In The 2016 Presidential Election Volume II of II*, www.justice.gov/storage/report_volume2.pdf.

Newsome, Gavin, speaker. *California Gov. Gavin Newsom's First State of the State Address (FULL) | NBCLA. YouTube*, NBCLA, 2 Feb. 2019, www.youtube.com/watch?v=R-IQthFnjBI.

Newton, Casey. "Read the Full Transcript of Mark Zuckerberg's Leaked Internal Facebook Meetings." *The Verge*, The Verge, 1 Oct. 2019, www.theverge.com/2019/10/1/20892354/mark-zuckerberg-full-transcript-leaked-facebook-meetings.

Official Journal of the European Union, L, no. 119, 4 May 2016, eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

"Overall Tobacco Trends." *American Lung Association*, www.lung.org/our-initiatives/research/monitoring-trends-in-lung-disease/tobacco-trend-brief/overall-tobacco-trends.html.

Palfrey, John G., and Urs Gasser. *Born Digital: How Children Grow up in a Digital Age*. Basic Books, 2016.

Park, Yong Jin, et al. "The Structuration of Digital Ecosystem, Privacy, and Big Data Intelligence." *American Behavioral Scientist*, vol. 62, no. 10, 2018, pp. 1319–1337., doi:10.1177/0002764218787863.

"Political Content." *Twitter*, Twitter, 2019, business.twitter.com/en/help/ads-policies/prohibited-content-policies/political-content.html.

"Political Content." *Twitter*, Twitter, business.twitter.com/en/help/ads-policies/prohibited-content-policies/political-content.html.

Pop, Doc. *What Is the CCPA and How Does It Compare to GDPR? YouTube*, YouTube, 25 July 2018, www.youtube.com/watch?v=z6Kez7o6n0k.

Proctor, Robert N. "The History of the Discovery of the Cigarette–Lung Cancer Link: Evidentiary Traditions, Corporate Denial, Global Toll: Table 1." *Tobacco Control*, vol. 21, no. 2, 2012, pp. 87–91., doi:10.1136/tobaccocontrol-2011-050338.

Prokop, Andrew. "The Mueller Report, Explained." *Vox*, Vox, 18 Apr. 2019, www.vox.com/2019/4/18/18485602/mueller-report-findings-obstruction-russia-collusion.

"Public Record of Usernames Linked to State-Sponsored Disinformation Campaigns." *Help Center*, Tumblr, tumblr.zendesk.com/hc/en-us/articles/360002280214.

"Putin Turned Russia Election Hacks in Trump's Favor: U.S. Officials." *Reuters*, Thomson Reuters, 16 Dec. 2016, www.reuters.com/article/us-usa-trump-cyber-idUSKBN1441RS.

Reich, Robert, author. *Why We Need to Break Up Big Tech. YouTube*, YouTube, 24 June 2019, www.youtube.com/watch?v=ora9KUXR7DY.

Romano, Aja. "The Facebook Data Breach Wasn't a Hack. It Was a Wake-up Call." *Vox*, Vox, 20 Mar. 2018, www.vox.com/2018/3/20/17138756/facebook-data-breach-cambridge-analytica-explained.

Simon, Abigail, and Abby Vesoulis. "Here's Who Found That Russia Meddled in the 2016 Election." *Time*, Time, 16 July 2018, time.com/5340060/donald-trump-vladimir-putin-summit-russia-meddling/.

Sloan, Robert H., and Richard Warner. "Beyond Notice and Choice: Privacy, Norms, and Consent." *SSRN Electronic Journal*, Jan. 2013, doi:10.2139/ssrn.2239099.

Solove, Daniel J. *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet*. Yale University Press, 2008.

Solove, Daniel, and Paul Schwartz. "Notice and Choice: Implications for Digital Marketing to Youth." *Change Lab Solutions*, 2009, www.changelabsolutions.org/sites/default/files/documents/Notice_and_choice.pdf.

Spencer, Scott. “An Update on Our Political Ads Policy.” *Google*, Google, 20 Nov. 2019, www.blog.google/technology/ads/update-our-political-ads-policy/.

Stephens, John. “California Consumer Privacy Act.” *American Bar Association*, 2 June 2019, www.americanbar.org/groups/business_law/publications/committee_newsletters/bcl/2019/201902/fa_9/.

Sánchez, David, and Alexandre Viejo. “Privacy-Preserving and Advertising-Friendly Web Surfing.” *Computer Communications*, vol. 130, 2018, pp. 113–123., doi:10.1016/j.comcom.2018.09.002.

“California Consumer Privacy Act.” *California Consumer Privacy Act*, OAG, 28 June 2018. oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-proposed-regs.pdf.

“California Consumer Privacy Act (CCPA) Fact Sheet.” OAG, 2018. https://oag.ca.gov/system/files/attachments/press_releases/CCPA%20Fact%20Sheet%20%2800000002%29.pdf.

“The Universal Declaration of Human Rights.” *United Nations*, 10 Dec. 1948, www.un.org/en/universal-declaration-human-rights/.

Warren, Elizabeth. “(Facebook)+(from:Ewarren)+++(Privacy) - Twitter Search.” *Twitter*, Twitter, 24 July 2019, twitter.com/search?q=%28facebook%29%2B%28from%3Aewarren%29%2B%2B%2B%28privacy%29&src=typed_query.

Warren, Elizabeth. @Warren. “Big tech companies like Facebook have too much power over our economy, our society, and our democracy. And when they buy out their competition, they stifle innovation and face less pressure to protect our privacy. That's why we need to #BreakUpBigTech.” *Twitter*, 12 May. 2019, https://twitter.com/ewarren/status/1127697561115033606?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1127697561115033606&ref_url=https%3A%2F%2Fyesnoperhaps.weebly.com%2Ffinal-project-digital-privacy

Warren, Elizabeth. “Here's How We Can Break up Big Tech.” *Medium*, Medium, 11 Oct. 2019, medium.com/@teamwarren/heres-how-we-can-break-up-big-tech-9ad9e0da324c.

Weigend, Andreas S. *Data for the People: How to Make Our Post-Privacy Economy Work for You*. Basic Books, 2017.

White, Andrew. *Digital Media and Society: Transforming Economics, Politics and Social Practices*. Palgrave Macmillan, 2014.

Williams, Evan. “‘The Internet Is Broken’: @Ev Is Trying to Salvage It.” *The New York Times*, 20 May 2017, www.nytimes.com/2017/05/20/technology/evan-williams-medium-twitter-internet.html.

Zuckerberg, Mark / The Verge. “In Leaked Audio, Mark Zuckerberg Rallies Facebook against Critics and the US Government.” *The Verge*, The Verge, 1 Oct. 2019, www.theverge.com/2019/10/1/20756701/mark-zuckerberg-facebook-leak-audio-ftc-antitrust-elizabeth-warren-tiktok-comments.

Zuckerberg, Mark. “CNN Exclusive: Zuckerberg Apologizes.” *CNN*, 21 Mar. 2018, www.cnn.com/videos/cnnmoney/2018/03/22/facebook-zuckerberg-cambridge-analytica-long.cnnmoney.