Daniel Urke

Professor Feigenbaum, Anat Lior

CPSC 610: Topics in Computer Science and Law

15 December 2019

Reclaiming Privacy: Protecting User Data in the Digital World

Abstract

As companies like Facebook and Google gain control over the digital world, addressing the problem of data privacy becomes increasingly important. These large online service platforms generate massive collections of user data that earn the companies significant targeted advertising revenues in exchange for providing their service to the user for free. However, this business model requires intense surveillance of users and leads to the accumulation of data that could be misused. Law professors, computer scientists, and economists have all proposed solutions to this problem, each with strengths and weaknesses. Jack Balkin's information fiduciary framework argues that companies who handle user data have a duty of trust–similar to that between a lawyer and their client–to act in the interests of the users and should be regulated as such. Providing an alternative solution, Jaron Lanier and Glen Weyl propose that the digital world should form an intermediary negotiating layer, mediators of individual data, between the users who produce the data and the platforms that use it. In order to address the key limitation of company incentives in these proposed interventions, governments could instead require any free service using this targeted advertising model to offer an optional paid service where the user would pay to have no data collected about them. Ultimately, all of these solutions have considerable drawbacks. Thus, a modification of Balkin's idea that regulates the end use of the data is the most likely proposal to begin to address the issue of user privacy.

The Problem

On election day, a randomly selected Facebook user scrolls past a post where they can announce that they had voted. Accompanying this post was a link to find polling places and profile pictures of friends who announced that they had voted. This seemingly innocuous push reminds the user to go vote, so they look up their polling location and after returning, push the button to notify their friends they had done their civic duty. This real scenario was part of a study of 61 million Facebook users during the 2010 US congressional elections. Cross referencing the users who were shown this post with public voting records, the study found that users who received a reminder to vote were 0.39 percent more likely to vote than the control group who did not see any post. The study ultimately concluded that the post had mobilized 60,000 voters.[1]

But what if this Facebook user was not selected at random? What if, in a closely contested election, Facebook used all of the data it collects for targeted advertising to instead only show this message to users expected to vote in a way that aligns with Facebook's political views? Facebook has proven they can accurately identify their users' political leanings and this "I Voted" post could be used to mobilize voters in a biased manner.[2] This is the situation that Johnathan Zittrain calls "digital gerrymandering" and he identifies it as just one of the possible abuses of the data that Facebook collects for targeted ads.[3]

This scenario illustrates a fundamental concern about user privacy, more specifically the possibility that tech companies who offer "free" services could abuse the data that they collect.

[1] Bond, Robert M et al., "A 61-million-person experiment in social influence and political mobilization"
[2] Jeremy Merill, "Liberal, Moderate, or Conservative? See How Facebook Labels You"
[3] Jonathan Zittrain, "Facebook Could Decide an Election Without Anyone Ever Finding Out"

Many people have identified targeted ads as the most pressing issue regarding the massive collection of user data. They say that targeted advertising can lead to numerous problems such as racial discrimination in housing and employment advertisements[4] or pushing "payday loans" to people identified as emotionally and financially vulnerable.[5] While targeted advertisements can certainly be problematic in their own right, the data used to create them opens the door to privacy and data abuses. This is what makes tech companies prime targets for data breaches and provides the impetus for big data projects like Facebook's DeepFace facial recognition program.[6] "Pervasive surveillance" is their business model and it is how they offer their platforms for "free."[7] The service is not the product, the user is.

Proposed Solution I: Jack Balkin's Information Fiduciary Framework

One solution that has gained traction lately is Yale Law Professor Jack Balkin's suggestion to model tech companies that monetize user data as "information fiduciaries." A fiduciary relationship is a special contract where one party has "an obligation to act in a trustworthy manner in the interest of another."[8] Fiduciaries have two basic duties. The first is a duty of care where the fiduciary must "act competently and diligently so as not to harm the interest of the… client." Second, and more important for online service platforms according to Balkin, fiduciaries "must… act in their clients' interests."[9] An information fiduciary is a fiduciary who has "special duties with respect to personal information that they obtain in the course of their relationships with their clients."[10] Both lawyers

[4] David Dayen, "Ban Targeted Advertising"
[5] Jonathan Zittrain, "How to Exercise the Power You Didn't Ask For"
[6] Yavin Taigman et al., "DeepFace: Closing the Gap to Human-Level Performance in Face Verification"
[7] Lina Kahn et al., "A Skeptical View of Information Fiduciaries"
[8] Jack Balkin et al., "A Grand Bargain to Make Tech Companies Trustworthy"
[9] Jack Balkin, "Information Fiduciaries and the First Amendment"
[10] Ibid.

and doctors fall into this category, and, according to Balkin, user-data based companies like Google and Facebook do as well.

Balkin's central argument for why digital companies should be modeled as information fiduciaries makes four key points. First, Balkin claims that there is an information asymmetry typical to fiduciary relationships since "online service providers have lots of information about us, and we have very little information about them or what they can do with the information they have collected."[11] Second, users are relatively dependent on these companies so "we must hope that they will not misuse our confidences or let loose information about us in ways that will harm us."[12] Third, online service providers claim to have expertise in a certain service such as search engines who "purport to give us the information we need quickly and efficiently."[13] Lastly, these companies collect what they know to be sensitive data and so they "hold themselves out as trustworthy organizations who act consistent with our interests, even though they also hope to turn a profit."[14] For these reasons, Balkin claims that an information fiduciary relationship exists between the user and the company and it should be regulated as such.

Balkin simplifies his idea to claim that companies that collect data should not act like "con artists" whereby they gain the trust of their users to not disclose their information and then use that information in a way that goes against their users' interests, thus violating that trust and benefiting the company.[15] According to Jonathan Zittrain, who has worked closely with Balkin on this topic, an information fiduciary model would prevent "data from being used for purposes unrelated to the

[11] Jack Balkin, "Information Fiduciaries and the First Amendment"
[12] Ibid.
[13] Ibid.
[14] Ibid.
[15] Lindsey Barrett, "Confiding in Con Men: U.S. Privacy Law, the GDPR, and Information Fiduciaries"

expectations of the people who shared it." For example, in the Cambridge Analytica case a personality quiz was used to profile voters and influence their political opinions.[16]

Balkin asserts that this model means that companies should be held responsible when "they hold themselves out as trustworthy, and… encourage the disclosure of the personal information that places end-users in a vulnerable position."[17] But Balkin clarifies that they can also be held responsible for promises beyond the terms of service they agree to with customers. He claims they must be held to a reasonable standard of trust and that this is what will prevent behavior such as digital gerrymandering.[18] Essentially, the restrictions put in place by Balkin would regulate the end use of the data by the tech company.

Zittrain says that it would be ideal if companies were to voluntarily take on this fiduciary responsibility instead of being forced into it by legislation.[19] For inspiration, Zittrain looks to the Digital Millennium Copyright Act (DMCA) which simplified copyright laws on digital platforms. The DMCA outlined the guidelines for notice and takedown on digital platforms like YouTube. Platforms that comply with the guidelines are promised to be protected from copyright infringement.[20] Zittrain proposes a Digital Millennium Privacy Act that would standardize privacy rules across the nation, which currently vary from state to state, making it difficult for companies to comply. In return, companies would accept the duties of the fiduciary relationship.[21]

Issues with Proposed Solution I: A Conflict of Interests

[16] Jonathan Zittrain, "How to Exercise the Power You Didn't Ask For"
[17] Jack Balkin, "Information Fiduciaries and the First Amendment"
[18] Ibid.
[19] Jonathan Zittrain, "How to Exercise the Power You Didn't Ask For"
[20] Jack Balkin et al., "A Grand Bargain to Make Tech Companies Trustworthy"
[21] Ibid.

The information fiduciary model has gained significant popularity recently. In academia it has received little to no scrutiny and members of Congress have expressed bipartisan support for the proposed framework.[22] Even Mark Zuckerberg said, "the idea of us [Facebook] having a fiduciary relationship with the people who use our services is intuitive."[23]

However, Lina Kahn and David Pozen caution skepticism regarding this increasingly supported idea. Kahn and Pozen's critique is essentially that Balkin's proposal would require tech companies to choose between their fiduciary duties to their shareholders or those to their users. According to these critics, "Facebook has a strong economic incentive to maximize the amount of time users spend on the site and to collect and commodify as much user data as possible."[24] Reforms that would benefit their users, such as making it less addictive, increasing personal privacy, and decreasing the amount of data third parties have access to, all would cut into Facebook's profits and not be in the interest of shareholders.[25] Kahn and Pozen point out that in numerous cases the courts have said that public companies have a duty to their shareholders above all others.[26]

The relationship between an online service provider and a user is fundamentally different from the relationship that doctors have with their patients. The information a doctor collects from a patient is simply a by-product of offering their service, whereas for online service providers, user data is their primary form of income.[27] Kahn and Pozen also point out that this model is vague on the substantive legal duties that fiduciaries would take on and proposes no framework for enforcing those duties. In the end, the fiduciary model is appealing because it is intuitive and simplistic, but it

[22] Lina Kahn et al., "A Skeptical View of Information Fiduciaries"
[23] "At Harvard Law, Zittrain and Zuckerberg Discuss Encryption, 'Information Fiduciaries' and Targeted Advertisements"
[24] Lina Kahn et al., "A Skeptical View of Information Fiduciaries"
[25] Ibid.
[26] Ibid.
[27] Ibid.

does not address the fundamental issue that online service companies make their money from collecting and monetizing user data.

Proposed Solution II: Lanier and Weyl's Mediators of Individual Data

Jaron Lanier and Glen Weyl's propose mediators of individual data (MIDs) to bridge the "yawning gap between big tech platforms and the individuals they harvest data from."[28] MIDs are an important part of their overall concept of "data dignity," which is essentially a digital society in which users are paid for the data they generate. They propose these MIDs as intermediaries who would negotiate data royalties, represent users with collective bargaining, and provide legal, accounting, and payment support to their members.[29] They envision a marketplace of MIDs that represent all the different types of producers of data. Each MID can make its own set of rules and in this way there will be some MIDs that value privacy over earnings from data, and others who prioritize selling data.[30] Individuals will belong to multiple MIDs and MIDs will compete for members which will lead MIDs to compete to best represent the preferences of individuals in the digital world.[31]

Lanier and Weyl outline a number of baseline requirements for MIDs. The first and foremost is that from the beginning MIDs will have a "true fiduciary" duty to the individuals who create data. They resolve any possible conflicts of interest by making this an "exclusive and overriding" duty to serve the "true best interests of data creators."[32] For example, they claim MIDs

[28] Jaron Lanier et al., "A Blueprint for a Better Digital Society"
[29] Ibid.
[30] Jaron Lanier, "Jaron Lanier Fixes the Internet"
[31] Jaron Lanier et al., "A Blueprint for a Better Digital Society"
[32] Ibid.

should not be set up to make all of their revenue from fees proportional to the volume of data they sell for their members because this would be no different than the problem they aim to solve, MIDs would then try to maximize selling member data at any cost. As a result, and in agreement with Lina Kahn and David Pozen, businesses whose primary revenue comes from advertisements like Google and Facebook cannot be MIDs because they have an inherent conflict of interest.[33]

Another notable requirement is that MIDs "must not allow data… to be permanently sold or alienated from the control of its members." Lanier and Weyl call this "inalienable provenance" and it means that MIDs should prevent buyers from accessing data beyond a specific use, essentially selling the data for a single use.[34] When this is not possible, the data should be marked so that the creator can demand a share of future revenue or refuse use altogether.

The last requirement for MIDs relating to privacy is what they term "cognitive realism," which means that MID members should not have to make overly complex decisions about their privacy nor be presented with onerous terms of service. They propose a simple knob where an individual can control the flow of data from their smartphone ranging from completely private (no selling data) to completely public (selling maximum data) as an example of a simple choice that would allow "a great many decisions [to] be compressed into a single parameter."[35]

Lanier and Weyl claim that MIDs will "reverse current trends in the information economy" where individualism has "paved the way for the rise of increasingly concentrated platform power." The requirements they lay out for MIDs would ensure that members are treated fairly and the large variation would allow data creators to express their preferences, selecting MIDs that are consistent

[33] Jaron Lanier et al., "A Blueprint for a Better Digital Society"
[34] Ibid.
[35] Ibid.

with their interests. In turn, MIDs will ensure that data buyers like advertisers are responsibly using their members' data. They claim that this is the only viable solution "yet articulated for the problem of excessive, erratic, and unsustainable power concentration on digital networks."[36]

Issues With Proposed Solution II

While this proposed solution certainly sounds like a simple solution that will lead to a bright future, there are three main issues that threaten it.

First, there are a number of technologies required for the creation of this "digital dignity" and MIDs. Chief amongst these is a technology to track data generated by a user through all of the machine learning and identify how much value it contributed to the conclusion.[37] While advances in differential privacy have made it increasingly possible to separate the control of the underlying data and that data's use for AI, Lanier admits that "fresh engineering" will be required to implement "payments, security, and provenance."[38]

In addition to the concerns over the current feasibility of the technology, it is not clear how the MIDs will function as an intermediary between the users and the platforms who would be paying for their data. Will MIDs prevent their members from using certain services until they have negotiated a deal with the platform? And how will MIDs be able to effectively ensure that data buyers are properly handling the data? Will they not face the same information imbalance that their individual members face? How will members be able to verify that MIDs are getting the maximum

[36] Jaron Lanier et al., "A Blueprint for a Better Digital Society"
[37] Jaron Lanier, "Jaron Lanier Fixes the Internet"
[38] Jaron Lanier et al., "A Blueprint for a Better Digital Society"

value for their data?[39] All of these are concerns about the specifics of MIDs that would need to be resolved.

The second main concern is an overall lack of incentive; platforms, MIDs, and data generators all will have to participate in the system in order for it to work. For platforms, Lanier claims that they will be incentivized to enter into the system because, although their share of the profits will decline, they will receive larger net profit since the "overall economy will grow so much that the tech companies will grow more than they would have otherwise."[40] No business would ever decrease their own market share to bet on the fact that the economy will grow more as a result. To achieve this result the online service providers would have to be regulated.

It is also not clear how MIDs will cover the cost of their operations. Lanier and Weyl mention that MIDs will be groups of volunteers. However, with data producers being members of so many different MIDs, it is impossible to think that they will be able to effectively do the "routine accounting, legal, and payment duties" of the MIDs on a volunteer basis. Thus, they will need to be professional organizations. Yet, Lanier and Weyl eliminate a structure where MIDs are paid as a portion of the revenue brought in from selling members' data, claiming that it will incentivize MIDs to sell as much data as possible at the expense of their members' interests.[41] Additionally, paying MIDs a flat rate does not seem feasible since this will not incentivize MIDs to get the maximum value for the data they have. How MIDs will be paid to represent their members remains an open problem for Lanier and Weyl's solution.

[39] Joshua Adams, "Getting Cash for Our Data Could Actually Make Things Worse"
[40] Jaron Lanier, "Jaron Lanier Fixes the Internet"
[41] Jaron Lanier et al., "A Blueprint for a Better Digital Society"

The last incentive problem is that of the users. It may seem like no user will refuse getting paid for their data, but Christopher Sprigma, a law and economics professor at NYU, refutes Lanier and Weyl's claim that a family of four could make 20,000 dollars in a year and thinks it is just as possible that it would be "only enough to buy you an occasional beer."[42] Sprigma also points out that unaccounted for transaction costs such as contracting, payment infrastructure, and termination fees will reduce the total amount that reaches the person who sold their data.[43]

The third and final concern is one of inequality. If data becomes commodified, the data of some users will become more valuable than others because advertisers, for the most part, will want to pay more for data about wealthier people who are more likely to have the disposable income to pay for their product. This will only "exacerbate inequality between users based on their wealth" as wealthy users are paid more to be advertised to.[44]

The feasibility of the MIDs is lacking, and even if it were possible from both a technical and business perspective, it is unclear whether all of the stakeholders would be properly incentivized and also seems that MIDs would simply increase inequality.

Proposed Solution III: An Option for Paid Services

Both of the solutions above fail to resolve the fundamental business equation. One solution that does is to regulate any online platform that offers a "free" service in exchange for data collection to have an option where users can pay for the service and not have their data collected. Companies like Facebook and Google would still be able to sell ads that are shown to these users, just not targeted

[42] Joshua Adams, "Getting Cash for Our Data Could Actually Make Things Worse"

[43] Ibid.

[44] Ibid.

ads. Users would cover the difference in value between the targeted ads and the general ads if they chose to pay for the service.

There would certainly be some regulatory hurdles to pass, such as getting the initial regulation in place and making sure that the price companies are charging is fair.[45] Even with these regulatory challenges, the greatest advantage of this solution is its feasibility. It does not have the technical challenges that MIDs do and, because it provides an additional source of revenue for the company collecting the data, it is a solution that would not make companies choose between their users and profits.

The important metric for this solution is average revenue per user (ARPU) which is used to measure how much money companies make per user. In 2018 Facebook's global yearly ARPU was 25 dollars while Amazon's for advertising (to exclude things like prime memberships) was 15 dollars. [46] Google's ARPU was much higher at 137 dollars per year globally.[47] However, Google does not provide a breakdown of their revenue by service so this number includes all Google services ranging from ads on Search and YouTube to revenue from their mobile apps and "Google Play."[48] Breaking it down, YouTube had a global ad revenue of 9.13 billion dollars in 2018.[49] At 2 billion users, this means the ARPU for YouTube ads is a much more manageable 4.60 dollars per year globally.[50] These statistics provide an example of what users could potentially expect to pay for online services. In addition, these prices would be discounted by the platforms still running non-targeted ads.

[45] Stacy-Ann Elvy, "Paying for Privacy and the Personal Data Economy"
[46] Frederic Filloux, "The ARPUs of the Big Four Dwarf Everybody Else"
[47] Ibid.
[48] J. Clement, "Google: Revenu Distribution 2001-2018, by source"
[49] J. Clement, "Global YouTube net advertising revenues 2016-2020"
[50] "YouTube by the Numbers"

Ultimately, the choice would be up to the user who would have to decide if this fee for a non-targeted ad service would be worth the increased privacy.

Issues with Proposed Solution III

The main issue raised with pay-for-privacy models, as their opponents call them, is that they do not solve the underlying privacy problem for everyone, just for the people who can afford to pay the privacy fee.[51] This essentially gives the illusion of choice, where many users would not be able to afford the private option while companies would be able to point to this "choice" as being made by the user.[52]

Another concern is that users will not end up choosing to pay for privacy, even if they have the ability to. When polled, only 25 percent of Americans would prefer to start paying a monthly subscription fee for Google and Facebook to stop them from collecting their data.[53] This is in contrast to the 80 percent of Americans who said they would "like Google and Facebook to collect less of their data."[54] This shows that people generally want privacy but also want their online services to remain free, and when given a choice between the two, will tend to give up their privacy. Factoring in that people will still see non-targeted ads, many users will not be able to tell the difference in their experience and will have a difficult time justifying the privacy fee they are paying because they are used to the service being free.

Also, a US-specific concern is that ARPUs limited to users in the US and other developed countries are consistently higher across all services. For Facebook, the yearly ARPU in the US and

[51] Bryce Craig, "Post-Privacy: Who Invited the Pay-for-Privacy Economy?"
[52] Stacy-Ann Elvy, "Paying for Privacy and the Personal Data Economy"
[53] Anthony Spadafora, "Americans Reluctant to Pay for Privacy"
[54] Ibid.

Canada is 112 dollars.[55] While this may make it easier for people in developing countries to afford the privacy fee, it means that even fewer users in the US will opt for the paid privacy version.

Other Proposed Solutions of Note

The proposed solutions covered above are not exhaustive.[56] Others worth mentioning include the break up of tech companies and a Chrome extension that aims to educate users.

Democratic presidential candidates such as Senator Elizabeth Warren have proposed using anti-trust law to break up big tech companies to improve privacy for individual users by increasing competition among companies on all issues, including that of privacy.[57] However, experts argue that this would actually make privacy and security worse. Large companies like Facebook have more resources to spend on security, and data breaches affect smaller firms like Under Armour and Caribou Coffee as well as large firms.[58]

There are also some technical approaches to the issue like "Terms of Service; Didn't Read" (ToS;DR) which is a Chrome extension that rates websites' terms of service and notifies the user of the rating and potentially problematic clauses in the terms of service. While informative, the ratings are obtained through crowd sourcing and verified by ToS;DR so only the most popular websites are rated.[59] This is a great way to start informing users of the terms of service they are agreeing to, but its limited scope is a major drawback.

[55] Frederic Filloux, "The ARPUs of the Big Four Dwarf Everybody Else"

[56] Both the EU's GDPR and the California Consumer Privacy Act are not covered in the scope of this essay. GDPR aims to solve the problem of data breaches at companies that store personal data, not the actual use of that data by the companies. The CCPA does attempt to solve the issue of privacy but its provision that users be able to opt out of the selling of personal data is still being clarified and would likely meet more resistance from tech companies if introduced nationwide.

[57] Elizabeth Warren, "Here's how we can break up Big Tech"

[58] Michael McLaughlin, "Breaking Up Big Tech Would Not Make Consumer Data More Secure"

[59] "Terms of Service; Didn't Read"

What is to Be Done?

The significant issues with all three of these proposals are a testament to the challenge of user privacy on online platforms. While the option for the private paid service would be the easiest to implement, Balkin's proposal to regulate the end use of the data, with alterations to avoid conflicts of interests when considering data collectors as fiduciaries to their users, comes closest to solving this problem.

Lanier and Weyl's MID and "data dignity" solution appears impressive but is not currently possible both from a technological and business perspective. Both the incentives for the stakeholders in the system (platforms, MIDs, users) and how the MIDs will effectively bargain for their users is unclear.

Offering users the option to pay for a service and not have their data collected would be the simplest solution to implement immediately. However, the preliminary polling of users regarding how much they are willing to pay for their privacy indicates that most will end up not paying for this privacy and just accept the data collection. Additionally, concerns over protecting only the privacy of those who can afford the fee would prevent this solution from gaining enough support to be implemented across the country.

The fiduciary model proposed by Balkin has its drawbacks as well. Balkin advertises the fact that Facebook, more specifically Mark Zuckerberg, is open to the idea of modeling online service companies as fiduciaries. However, this should actually be a cause for concern. Facebook does not intend to fundamentally change its business model and hence anything they sponsor will allow them to continue maximizing the amount of data they control in order to continue to grow their ad revenue. This idea is fundamentally at odds with the interests of their users and if Facebook has to choose between their users' interests and that of their shareholders, they will choose their shareholders every time.

Despite these concerns, the idea of regulating the end use of the data is appealing because it is a compromise. Abuses such as the "digital gerrymandering" could be prevented while some fair uses of data collected by social media platforms could still allow them to generate revenue. Where to draw the line in these regulations would have to be determined by a regulatory body such as the FTC and the punishments would have to be severe enough to actually disincentivize violating those regulations. These end use regulations could be coupled with the continued option to opt out of data collection altogether for extra privacy-conscious users willing to pay the price.

The issue of user data privacy for online services will continue to be of importance as people increasingly rely on these platforms, making it critical that solutions continue to be developed.

References

Adams, Joshua. "Getting Cash for Our Data Could Actually Make Things Worse." *Medium*, OneZero, 25 Oct. 2019, onezero.medium.com/getting-cash-for-our-data-could-actually-make-things-worse-3793c52ec7e5.

"At Harvard Law, Zittrain and Zuckerberg Discuss Encryption, 'Information Fiduciaries' and Targeted Advertisements - Harvard Law Today." *Harvard Law Today*, Harvard Law Today, 2019, today.law.harvard.edu/at-harvard-law-zittrain-and-zuckerberg-discuss-encryption-information-fiduciaries-and-targeted-advertisements/.

Balkin, Jack. "Information Fiduciaries and the First Amendment." *UC Davis Law Review*, vol. 49, no. 4, Apr. 2016, lawreview.law.ucdavis.edu/issues/49/4/Lecture/49-4_Balkin.pdf.

Balkin, Jack M, and Jonathan Zittrain. "A Grand Bargain to Make Tech Companies Trustworthy." *The Atlantic*, The Atlantic, 3 Oct. 2016, www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346/.

Barrett, Lindsey. "Confiding in Con Men: U.S. Privacy Law, the GDPR, and Information Fiduciaries." *Seattle University Law Review*, vol. 42, 2019. https://digitalcommons.law.seattleu.edu/cgi/viewcontent.cgi?article=2601&context=sulr

Bond, Robert M et al. "A 61-million-person experiment in social influence and political mobilization." *Nature* vol. 489,7415 (2012): 295-8. doi:10.1038/nature11421

Clement, J. "Google Revenue Breakdown by Source 2018." *Statista*, Statista, 9 August 2019, www.statista.com/statistics/266471/distribution-of-googles-revenues-by-source/.

Clement, J. "YouTube Global Net Advertising Revenues 2020." *Statista*, Statista, 7 May 2019, www.statista.com/statistics/289658/youtube-global-net-advertising-revenues/.

Craig, Bryce. "Post-Privacy: Who Invited the Pay-for-Privacy Economy?" *Medium*, The Startup, 28 May 2019, medium.com/swlh/post-privacy-who-invited-the-pay-for-privacy-economy-626aecaf53e9

Dayen, David. "Ban Targeted Advertising." *The New Republic*, 10 Apr. 2018, newrepublic.com/article/147887/ban-targeted-advertising-facebook-google.

Eline Chivot. "Paying Users for Their Data Would Exacerbate Digital Inequality." *Center for Data Innovation*, 11 Jan. 2019, www.datainnovation.org/2019/01/paying-users-for-their-data-would-exacerbate-digital-inequality/.

Filloux, Frederic. "The ARPUs of the Big Four Dwarf Everybody Else." *Medium*, Monday Note, 11 Feb. 2019, mondaynote.com/the-arpus-of-the-big-four-dwarf-everybody-else-e5b02a579ed3.

"Jonathan Zittrain and Jack Balkin Propose Information Fiduciaries to Protect Individual Privacy Rights." *Technology, Academics, Policy*, 28 Sept. 2018, www.techpolicy.com/Blog/September-2018/Jonathan-Zittrain-and-Jack-Balkin-Propose-Informat.aspx.

Khan, Lina and Pozen, David E., A Skeptical View of Information Fiduciaries (2019). Harvard Law Review, Vol. 133, pp. 497-541, 2019. Available at SSRN: https://ssrn.com/abstract=3341661

Lanier, Jaron. "Opinion | Jaron Lanier Fixes the Internet." *The New York Times*, 23 Sept. 2019, www.nytimes.com/interactive/2019/09/23/opinion/data-privacy-jaron-lanier.html.

Lanier, Jaron. *Who Owns the Future?*. New York, Simon & Schuster Paperback, 2014.

Lanier, Jaron, and Glen Weyl. "A Blueprint for a Better Digital Society." *Harvard Business Review*, 18 Oct. 2018, hbr.org/2018/09/a-blueprint-for-a-better-digital-society.

McLaughlin, Michael, and Daniel Castro. "Breaking Up Big Tech Would Not Make Consumer Data More Secure." *Itif.Org*, Information Technology and Innovation Foundation, 2019, itif.org/publications/2019/04/10/breaking-big-tech-would-not-make-consumer-data-more-secure.

Merill, Jeremy. "Liberal, Moderate or Conservative? See How Facebook Labels You." *The New York Times*, 23 Aug. 2016, www.nytimes.com/2016/08/24/us/politics/facebook-ads-politics.html.

Spadafora, Anthony. "Americans Reluctant to Pay for Privacy." *TechRadar*, 16 Jan. 2019, www.techradar.com/au/news/americans-reluctant-to-pay-for-privacy.

Taigman, Yaniv, et al. "DeepFace: Closing the Gap to Human-Level Performance in Face Verification." *Facebook Research*, 24 June 2014. https://research.fb.com/wp-content/uploads/2016/11/deepface-closing-the-gap-to-human-level-performance-in-face-verification.pdf?

ToS;DR Team. "Terms of Service; Didn't Read." *Tosdr.Org*, Terms of Service; Didn't Read, 2019, tosdr.org/.

Warren, Elizabeth. "Here's How We Can Break Up Big Tech." *Medium*, Medium, 8 Mar. 2019, medium.com/@teamwarren/heres-how-we-can-break-up-big-tech-9ad9e0da324c.

"YouTube By the Numbers." *YouTube*, 2019, www.youtube.com/about/press/.

Zittrain, Jonathan. “Facebook Could Decide an Election—Without You Ever Finding Out.” *The New Republic*, 2 June 2014, newrepublic.com/article/117878/information-fiduciary-solution-facebook-digital-gerrymandering.