The Maastricht Journal of Liberal Arts
2021, Volume Thirteen, pp. 63-77

FEDERAL TRADE COMMISSION V. FACEBOOK

Case Study of The Effects of Antitrust Laws on Consumers Data Privacy Protection

Authors: Cam Nghiem, Dominique Lopez, Austin Sievers

Abstract On December 9, 2020, the United States (U.S.) Federal Trade Commission (FTC) filed an antitrust lawsuit against Facebook. The lawsuit is an attempt by the U.S. government to regulate big-tech companies using antitrust laws after noticing the growing concerns of consumers' data privacy breaches. The use of antitrust laws to regulate consumers' data protection has been debated extensively by legal scholars; however, the debate focuses too much on theory and ignores the effectiveness of antitrust remedies. This paper looks at *Federal Trade Commission v. Facebook, Inc.* from both viewpoints of legal theory and practicality. It concludes that even though U.S. antitrust laws have possible jurisdiction over consumers' data privacy protection issues, their available legal remedies are not qualified to ensure consumers' data privacy protection.

1. Introduction

In recent years, Facebook has found itself caught in various scandals. In 2019, the United States (U.S.) Department Justice Special Counselor Robert Mueller reported how the Russian Internet Research Agency had used Facebook to interfere with the 2016 U.S. Presidential Election (p. 24). Ms. Yanghee Lee, a United Nations investigator of the Rohingya crisis, also cited Facebook as a tool to spread hate speech (Miles, 2018). Moreover, its biggest scandal is Cambridge Analytica, in which the voter-profiling firm Cambridge Analytica "harvested private information from the Facebook profiles of more than 50 million users without their permission" (Rosenberg et al., 2018, para. 4). After

the Cambridge Analytica data breach scandal, Facebook was criticized by the U.S. lawmakers.

To address the problem of Facebook and other companies' possible data misappropriations and data breach, the European Union (E.U.) adopted Regulation 2016/679, which is also known as the General Data Protection Regulation (GDPR), to expand the protection of E.U. citizens' data rights.[1] On the other hand, the United States has not adopted any regulations to strengthen its citizens' data rights. With the lack of data protection legislation at the federal level, the U.S. government must depend on other existing legislations to hold companies such as Facebook accountable for its mismanagement of users' data.

Antitrust, or competition legislation, has been nominated for this task (Tyagi, 2019a, p. 281). Hence, on December 9, 2020, the United States (U.S.) Federal Trade Commission (FTC) filed an antitrust lawsuit against Facebook at the U.S. District Court for the District of Columbia. The Commission accuses Facebook of "illegally maintaining its social networking monopoly through a years-long course of anticompetitive conduct" (Federal Trade Commission, 2020, para. 1). It argues that the lack of competition against Facebook has decreased the number of consumer choices regarding "the availability, quality, and variety of data protection privacy options for users, including, but not limited to, options regarding data gathering and data usage practices" (Federal Trade Commission v. Facebook, Inc.).

The previous argument implies that the FTC might have considered consumers' data privacy protection to be an antitrust issue, at least in this lawsuit against Facebook. However, the opinion might not be unanimous. Incumbent FTC Commissioner Noah Phillips claims that "using antitrust law to advance privacy protections ... 'will fail'" (Kendall, 2020, para. 3). In order to address this conflicted idea, this paper investigates the following question: to what extent are legal remedies provided by U.S. antitrust laws effective in ensuring consumers' data privacy protection of Facebook users?

In order to respond to the previous question, this paper views the issue using an interdisciplinary framework consisting of antitrust legal theory, economics, and ethics.

[1.] The GDPR (or Regulation 2016/679) expands the data protection of E.U. citizens by repealing the old Directive 95/46/EC and defining 'data portability' to address the problems posed by Facebook and the likes.

Essentially, the paper argues that even though U.S. antitrust laws have possible jurisdiction over consumers' data privacy protection issues, their available legal remedies, especially in *Federal Trade Commission v. Facebook, Inc.*, still cannot ensure consumers' data privacy protection due to the current antitrust analysis model of regulatory agencies and the winner-take-all nature of the personal social networking market.

The paper has four main sections. Section 2 argues that the problem of consumers' data privacy protection is under the jurisdiction of the current U.S. antitrust laws. Section 3 argues that forced divestiture of Facebook, interoperability, and forced data sharing are not effective antitrust remedies against consumers' data privacy protection problems due to the personal social networking services market's winner-take-all nature. Section 4 discusses concerns that are not addressed by antitrust remedies mentioned in section 3—the inconsistency of some antitrust remedies with the informational self-determination principle and the lack of universal enforcement of consumers' data privacy protection.

2. Data Privacy Protection and Antitrust Jurisdiction

On December 9, 2020, the Commission accused Facebook of violating Section 2 of the Sherman Act due to their alleged anticompetitive conducts to monopolize the personal social networking services market and therefore also Section 5(a) of the FTC Act. The Sherman Act of 1890 and the FTC Act of 1914 are the two foundational acts of U.S. antitrust laws. These antitrust laws can be broadly interpreted to consider consumers' data privacy protection as an antitrust issue for two reasons.

The first reason is that the Sherman Act and the FTC Act can be broadly interpreted due to their characteristics of being mainly developed via common law. U.S. antitrust laws are developed mainly via common law means because of the Sherman Act's broad language as courts must apply specific such a broad language into specific cases, such specification by-case is the common-law development of U.S. antitrust laws. In addition, the Sherman Act is also tied to the FTC act because "all violations of the Sherman Act also violate the FTC Act" (Federal Trade Commission, para. 5). Therefore, due to the Sherman Act's broad language, the U.S. antitrust laws as a whole have become broad and hence have been crafted through a common-law process. Being crafted through a common-law process means that the courts "shape rules applying the

Sherman Act's broad prohibitions through incremental trial and error" (Drivas, 2019, p. 1906). Thus, the courts can change their interpretation philosophy regarding antitrust laws. Such change was first observed in the 1970s with the rise of the Chicago School as a reaction to the robust interventionist antitrust regime at the time. The Chicago approach to antitrust laws is predicated on neoclassical economics, whose proponents believe in the "market efficiency and [have] skepticism toward government interference in the economy" (Drivas, 2019, p. 1909). This approach has remained dominant until now. It is evident that there was a shift in the past from the interventionist enforcement of antitrust laws to the current non-interventionist one. Such a shift confirms the possibility of a change in the interpretation of antitrust laws in the present, which might be a reaction to the current digital economy's personal social networking market and its consumers' data privacy protection issues.

Second, the Sherman Act and the FTC Act can be interpreted to address consumers' data privacy protection. The previous paragraph argues that antitrust interpretation can change in reaction to certain phenomena; this raises the question of how the current interpretation should change. Lee (2020) argues that the change in interpretation must start at antitrust law enforcement agencies. Currently, U.S. courts and antitrust law enforcement agencies follow the interpretation of the Chicago School, which argues that the purpose of antitrust law is to protect consumers by making the products the lowest price possible. Lee (2020) criticizes that such interpretation is too "strictly concerned with price-based consumer welfare and reject[s] the idea that the standard protects consumers from other seemingly non-economic goals like privacy and democracy" (p. 90). Indeed, if we look at Facebook's current personal social networking market, the services provided are free in terms of monetary price but cost customers their data privacy and security. By changing their interpretation and redefining consumer harms to include matters such as privacy and security and not just monetary costs, the U.S. courts and antitrust law enforcement agencies can better ensure customer protection for U.S. citizens.

In sum, antitrust laws can be broadly interpreted to consider consumers' data privacy protection as an indicator of antitrust issues. U.S. courts and antitrust law enforcement agencies can redefine consumer protection to address problems outside monetary costs such as consumers' data privacy protection in reaction to the current digital economy's personal social networking market.

3. Forced Divestiture, Interoperability, and Forced Data Sharing

While section 2 discussed the utilization of antitrust laws to address concerns of consumers' data privacy, sections 3 discusses legal remedies available in the current U.S. antitrust laws to address such concerns, which are (1) divestiture or reconstruction of Facebook's assets and businesses and (2) banning Facebook from imposing anti-competitive terms and conditions on access to its data. This section argues that the two aforementioned remedies are not effective against consumers' data privacy protection problems due to the winner-take-all nature of the personal social networking services market. To clarify, through divestiture or reconstruction of Facebook's assets, the FTC would require forced divestiture of Facebook, meaning that Facebook subsidiaries—for example, Instagram and WhatsApp—would be split up and made into their own companies again. Under the method of banning Facebook from imposing anti-competitive terms and conditions on access to its data, the FTC could require interoperability and forced data sharing. Requiring interoperability would mean that Facebook would have to ensure that users on other social networking platforms could access their Facebook friends on their other platforms (Kimmelman et al., 2019). Similarly, forced data sharing is described as:

> [E]very company above a certain size, say, those with more than a ten percent share of the market, that systematically collects and analyzes data would have to let other companies in the same market access a subset of its data. The larger a firm's market share, the more of its data others would be allowed to see. (Mayer-Schonberger et al., 2018, p. 53)

This section will examine the effectiveness of forced divestiture, interoperability, and forced data sharing regarding the protection of personal privacy.

If protecting consumers' data privacy is the ultimate goal, forced divestiture alone would not be effective because of the digital market's winner-take-all nature and the power that Facebook holds over it. The winner-take-all nature of the social networking market has been described as Schumpeterian competition; this is when firms compete *for* the market instead of *in* the market (Katz, 2020). Digital markets work like this because of positive network externalities where people rely on them to stay in touch with

family and friends, thus creating a network effect. The more active people on a platform, the more valuable the platform becomes for everyone else. The Schumpeterian competition encourages a concentration of data at the top companies and might create a situation where people do not care that their data is being used if they get a more efficient product (Kimmelman et al., 2019; Lamoreaux, 2019; Mayer-Schonberger et al., 2018). Given this dynamic, Facebook Blue (Facebook without subsidiaries) alone would still dominate a significant portion of the social networking market and would have no incentive to change its privacy policy. The digital data market operates best when companies have broad access to data; combined data sets drive innovation and make a product more efficient (Ohlhausen et al., 2015; Mayer-Schonberger et al., 2018). Thus, forced divestiture alone would not help other companies grow to challenge the existing dominant company because they would not have access to that data; in the end, this would have the effect of preserving the existing market hierarchy while doing little to address concerns over competition (Mayer-Schonberger et al., 2018). Even after forced divestiture, Facebook Blue would still hold a massive data advantage over its next closest competitor given its size. As can be seen from these problems, forced divestiture would limit Facebook's market power, but this remedy would be ineffective in creating the conditions for another company to challenge Facebook.

Because of the nature of the personal social networking market, the only way to create a competitive environment is through forced data sharing or interoperability. A core aspect of Facebook's business model relies on its ability to leverage its products to harm competitors. This is done by telling software developers and third parties that they can only connect their products to Facebook if they agree not to copy Facebook's business model or work with Facebook's competitors (Federal Trade Commission v. Facebook, Inc.). Through interoperability and forced data sharing, the market could become competitive again with smaller companies having the ability to access the larger companies' data; by making Facebook interoperable with other social networks, it removes the leverage that Facebook has been using to keep the market anti-competitive. The problem with this solution is that it would require personal data to be spread around to other companies, potentially putting data privacy at risk. Furthermore, given the globalized market and the different data privacy regulatory regimes (GDPR or CCPA), it would take significant work to ensure a worldwide data privacy standard.

In addition to concerns over increased data vulnerability, it is not immediately apparent that it would be in a company's best interest to protect data privacy, even if there was some demand in the market for it. Competition law would say that if there were a market for a company with better privacy protections, consumers would reward their business to the company that prioritizes privacy. The issue with this line of reasoning is that if a company does not look at data, their product will not be as efficient and will have a smaller market (Colangelo & Maggiolino, 2018). Such an incentive leads to the company that abuses privacy rights maintaining its dominant market position (Rancati, 2019). If banning Facebook from imposing anti-competitive conditions on access to its data were to be useful in protecting data privacy, special laws would need to be enacted to ensure personal data protection. While these solutions are a step in the right direction and address the need for increased competition in the market, without further regulations to ensure data privacy protection, interoperability, and forced data sharing will not be enough.

In summary, it is clear that the remedies of forced divestiture, interoperability, and forced data sharing on their own are not sufficient to protect the data privacy of Facebook users. As shown above, forced divestiture would be ineffective at creating competition without interoperability or forced data sharing. While these two methods in conjunction may increase competition in the market, there are serious privacy concerns when it comes to interoperability and forced data sharing. Section 4 argues why creating separate federal data privacy legislation would be more effective.

4. Issues Unresolved by Current U.S. Antitrust Remedies: The Informational Self-Determination Principle & Universal Enforcement

If neither forced divestiture nor interoperability and forced data sharing effectively ensure consumers' data privacy protection, a different solution needs to be found. This section argues that it is more efficient for the U.S. government to create separate federal legislations to address the problems of consumers' data privacy protection instead of depending on the current U.S. antitrust remedies[2]. This is because current remedies are

[2.] At the time of writing, the US House of Representative has proposed five antitrust bills to tackle the issues of Facebook and the likes (Competition Policy International, 2021).

unable to uphold the ethical principle of informational self-determination or enforcing consumers' data privacy protection.

To understand why separate federal legislation is more efficient, it is essential to explain the concept of context integrity framework. Contextual integrity is an ethical theory of privacy, claiming that whether an action is a privacy violation depends on the following factors:

> the nature of the situation, or context; the nature of the information in relation to that context; the roles of agents receiving information; their relationships to information subjects; on what terms the information is shared by the subject; and the terms of further dissemination. (Nissenbaum, 2004, p. 155)

This essentially states that data should only be disclosed according to the terms or contexts established and agreed by the users. These contexts comprise five main parameters: (1) data subject, (2) sender, (3) recipients, (4) the type of data (or attribute), and (5) transmission principle (Shvartzshnaider et al., 2019, p. 163). To illustrate, when one agrees that Facebook can have one's contact information by importing it from one's iPhone, they are both the data subject and the sender, Facebook is the recipient, contact information is the type of data, and the transmission principle is importation of data from one's iPhone. In addition to the concept of contextual integrity, there is also the ethical concept of informational self-determination. Informational self-determination is defined as the ability for users to make their own decisions on disclosing their personal data (Roosendaal, 2011). The concepts of the contextual integrity framework and the informational self-determination principle are intertwined. If information is used according to the contextual integrity framework, it means the users' right to informational self-determination is respected.

In this light, the proposed antitrust remedies of interoperability and forced data sharing go against the ethical principle of informational self-determination mentioned above. First, in terms of interoperability, when Facebook shares users' data to other platform apps, users no longer control what information about them gets shared (Tyagi, 2019a). Instead, they are given a chance to accept a transmission principle, such as connecting their Facebook profile, but that does not specify the extent to which data is

shared to another platform. If the recipient does not clarify what data gets shared from a user to another platform, users are forced to two extremes. Users must either accept the sharing of data information among platforms completely or decline thus impacting the platform's possibility to work efficiently. Also, having Facebook cut down their network benefit to let other companies (such as Snapchat or Twitter) find your Facebook friends on their platforms would mean that the sender/user has to give consent to the recipient. When the sender gives consent to another platform app to sync their contacts or connect their Facebook profile, they agree that Facebook can use their specific request information as an attribute to share with the platform. When the sender agrees to a particular attribute to be shared, they are aware that they have only given consent to what was asked from them on the platform and not beyond the transmission principal phrase. However, to protect users' data privacy, "interoperability cannot give rise to the access or use of any data via another information system or give access to more data than is needed" (European Data Protection Supervisor, n.d., para. 1). While the idea behind interoperability appears innocent in data misuse, it does not necessarily aim at protecting users' data since it has to be shared with other companies without the due process of obtaining users' consent. In this case, informational self-determination is not in the sender's hands because they do not have full disclosure of how their data gets used. Users are left in the dark about what third parties or other platforms their data will be exchanged or shared. Second, in terms of forced data sharing, the sender (individual) must share any information that the terms and conditions request to the receipt (such as Facebook). Not only is the attribute, such as contact information, and transmission principle (such as syncing an address book from a device) forcibly shared to Facebook but also possible third parties. The coercive nature of data sharing, which interoperability encompasses, does not give users a choice or say in how their data is being utilized. Users should be able to control certain information that they deem unnecessary to share with Facebook and firms alike. Third, users cannot give full consent if they are not fully informed about how their data will be utilized or shared through the market. Without the individual's consent, the data should not be mistreated in other contexts. For data privacy to seriously be considered, a breach in informational flow such as using the users' data attribute without specifying data use means that the user was not given the possibility of giving consent to the data accumulation process.

In addition to their inconsistency with the ethical privacy principle of informational self-determination, U.S. antitrust remedies are also ineffective due to their lack of universal enforcement of consumers' data privacy protection. First, it must be understood that there are significant similarities between the enforcement of the U.S. antitrust laws and E.U. competition laws. Many major U.S. antitrust legislations can find the same legalese in their E.U. counterparts:

> As most antitrust practitioners are no doubt aware, §§1 and 2 of the Sherman Act, passed in 1890, cover largely the same ground as Articles 81 and 82 of the Treaty of Rome [Articles 101 and 102 of the Maastricht Treaty]: Section 1 prohibits concerted action in unreasonable restraint of trade and §2 prohibits anticompetitive conduct that contributes to the acquisition or preservation of monopoly power. Section 7 of the Clayton Act is roughly comparable to the EC Merger Regulations[3] [footnote added]; it prohibits mergers and acquisitions the effect of which may be "substantially to lessen competition, or [which] tend to create a monopoly." (Ginsburg, 2005)

As an established monopoly in the personal social networking services market, Facebook is under the scrutiny of the U.S. Federal Trade Commission and the European Commission. However, the desire for the sustainability of consumers' data privacy protection raises the question of the enforcement of data protection at companies that *are not* the subjects of U.S. antitrust or E.U. competition legislation. In the E.U., this problem is resolved with Regulation 2016/679, or the General Data Protection Regulation (GDPR). While E.U. competition legislation only applies to dominant service providers, the GDPR "can be enforced against all data controllers irrespective of their size and market shares" (Vanberg & Ünver, 2017, p. 14). In the U.S., however, due to the similarity regarding the subject of the laws between U.S. antitrust and E.U. competition legislation, it can be deduced that the U.S. FTC will not enforce antitrust remedies against *all* violators of consumers' data privacy protection unless such violations are anti-competitive measures for said violators to acquire or preserve monopoly. The reason

---

3. It must be noted that there is only one EU Merger Regulation. The current EU Merger Regulation, as of the time of writing, is Regulation 139/2004 is the 'successor' of EEC Regulation 4064/89.

is that even with a broad interpretation of antitrust laws as argued in section 2, privacy concerns are still one among many factors, *and not the determining factor*, that the FTC considers whether to file antitrust lawsuits; the pure presence of privacy concerns are not sufficient for the FTC to initiate such proceedings. This means the U.S. government currently has no legal power to punish non-monopolies for violations of consumers' data privacy protection[2]. This situation begs the creation of a U.S. equivalence of the GDPR, which would guarantee users' data privacy without the need for forced data sharing or interoperability.

In sum, it is more efficient for the U.S. government to create separate federal guidelines to address consumers' data privacy protection problems instead of depending on the current U.S. antitrust remedies. The proposed antitrust remedies of interoperability and forced data sharing go against informational self-determination's ethical privacy principle. Moreover, the available U.S. antitrust remedies are also ineffective due to their lack of universal enforcement of consumers' data privacy protection for all companies regardless of sizes.

5. Conclusion

This paper has examined two of the antitrust remedies that the U.S. government has contemplated in its lawsuit against Facebook: (1) divestiture or reconstruction of Facebook's assets and businesses; and (2) banning Facebook from imposing anti-competitive terms and conditions on access to data (Federal Trade Commission v. Facebook, Inc.). The paper respectively referred to these antitrust remedies as forced divestiture, interoperability, and forced data sharing.

The paper distinguishes between antitrust laws and its associated antitrust remedies. Indeed, with a broader interpretation, the current antitrust laws can include consumers' data privacy protection issues as an indicator of antitrust issues, allowing current antitrust laws to address data privacy protection problems. However, not all current antitrust remedies proposed by the U.S. government effectively address data privacy issues. Forced divestiture, interoperability, and forced data sharing are not effective due to the winner-take-all nature of the personal social networking services market; they are also inconsistent with the ethical principle of informational self-determination. Another problem is the lack of universal enforcement of consumers'

data privacy protection upon all companies regardless of sizes due to the main subject of U.S. antitrust laws being only big anti-competitive companies. For such reasons, it is more efficient for the U.S. government to create separate federal guidelines to address consumers' data privacy protection issues instead of depending on the current U.S. antitrust remedies.

References

Colangelo, G. & Maggiolino, M. (2018). Data accumulation and the privacy–antitrust interface: Insights from the Facebook case. *International Data Privacy Law, 8*(3), 224–239. https://doi.org/10.1093/idpl/ipy018

Competition Policy International. (2021). Democrats introduce 5 antitrust bills aimed at reining in big tech. Retrieved September 27, 2021, from https://www.competitionpolicyinternational.com/democrats-introduce-5-antitrust-bills-aimed-at-reining-in-big-tech/

Drivas, I. (2019). Liability for data scraping prohibitions under the refusal to deal doctrine: An incremental step toward more robust Sherman Act enforcement. *The University of Chicago Law Review*, *86*(7), 1901-1940. https://www.jstor.org/stable/26792620

European Commission. (n.d.) Data protection in the EU. https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

European Data Protection Supervisor. (n.d.) Interoperability. https://edps.europa.eu/data-protection/our-work/subjects/interoperability_en

Federal Trade Commission. The antitrust laws. https://www.ftc.gov/tips-advice/competition-guidance/guide-antitrust-laws/antitrust-laws

Federal Trade Commission. (2020). FTC sues Facebook for illegal monopolization. https://www.ftc.gov/news-events/press-releases/2020/12/ftc-sues-facebook-illegal-monopolization

Federal Trade Commission v. Facebook, Inc. (2020). Complaint for injunctive and other equitable relief (Public Redacted Version). *US District Court for the District of Columbia.* https://www.ftc.gov/system/files/documents/cases/1910134fbcomplaint.pdf

Ginsburg, D. (2005). Comparing antitrust enforcement in the United States and Europe. *Journal of Competition Law & Economics*, *1*(3), 427–439. https://doi.org/10.1093/joclec/nhi017

Katz, M. L. (2020). Big Tech mergers: Innovation, competition for the market, and the acquisition of emerging competitors. *Information Economics and Policy*, 100883. https://doi.org/10.1016/j.infoecopol.2020.10088

Kendall, B. (2020). FTC Commissioner: Antitrust enforcement isn't answer to tech privacy concerns. *The Wall Street Journal.* https://www.wsj.com/articles/ftc-commissioner-antitrust-enforcement-isnt-answer-to-tech-privacy-concerns-11580419657

Kimmelman, G. (2019). Models for platform governance. *Centre for International Governance Innovation*. https://doi.org/10.2307/resrep26127.10

Lamoreaux, N. (2019). The problem of bigness: From standard oil to google. *The Journal of Economic Perspectives, 33*(3), 94-117. https://www.jstor.org/stable/26732323

Lee, J. (2020). The Google-DoubleClick Merger: Lessons from the Federal Trade Commission's limitations on protecting privacy. *Communication Law and Policy, 25*(1), p. 77-103. https://doi.org/10.1080/10811680.2020.1690330

Mayer-Schonberger, V. & Ramge, T. (2018). Big choice for big tech: Share data or suffer the consequences. *Foreign Affairs, 97*(5), 48-54. https://www.foreignaffairs.com/articles/world/2018-08-13/big-choice-big-tech

Miles, T. (March 12, 2018). U.N. investigators cite Facebook role in Myanmar crisis. *Reuters*. https://www.reuters.com/article/us-myanmar-rohingya-facebook/u-n-investigators-cite-facebook-role-in-myanmar-crisis-idUSKCN1GO2PN

Nissenbaum, H. (2004). Privacy as Contextual Integrity. *Washington Law Review, 79*, 119-158. https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10

Ohlhausen, M. & Okuliar, A. (2015). Competition, Consumer Protection, And The Right [Approach] To Privacy. *Antitrust Law Journal, 80*(1), 121-156. https://www.jstor.org/stable/26411522

Rancati, L. & de Ghellinck, E. (2019). The intersection between Antitrust and Data Protection. Lessons from the Facebook/Whatsapp merger and the Bundeskartellamt's decision on Facebook's terms and conditions. *Faculté des sciences économiques, sociales, politiques et de communication, Université catholique de Louvain.*

Roosendaal, A. (2011). Facebook tracks and traces everyone: Like this! *Tilburg Law School Legal Studies Research Paper Series, 2*(9). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1717563

Rosenberg, M., Confessore, N. & Cadwalladr, C. (2018). How trump consultants exploited the Facebook data of millions. *The New York Times*. https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html

Shvartzshnaider, Y., Apthorpe, N., Feamster, N., & Nissenbaum, H. (2019). Going against the (appropriate) flow: A contextual integrity approach to privacy policy analysis. *Association for the Advancement of Artificial Intelligence*. https://nissenbaum.tech.cornell.edu/papers/Going%20Against%20the%20(Appropriate)%20Flow.pdf

Tyagi, K. (2019a). Big data and merger control. *Promoting Competition in Innovation Through Merger Control in the ICT Sector*, 265–303. https://doi.org/10.1007/978-3-662-58784-3_17

Tyagi, K. (2019b). Merger control in the EU and the UK. *Promoting Competition in Innovation Through Merger Control in the ICT Sector*, 113–130. https://doi.org/10.1007/978-3-662-58784-3_7

Tyagi, K. (2019c). Merger control in the US. *Promoting Competition in Innovation Through Merger Control in the ICT Sector*, 131–140. https://doi.org/10.1007/978-3-662-58784-3_8

Teachout, Z. (2020). *Break 'Em Up: Recovering Our Freedom from Big Ag, Big Tech, and Big Money*. Macmillan Publishers.

United States Department of Justice. (2019). Report on the investigation into Russian interference in the 2016 Presidential Election (Public Redacted Version). https://www.justice.gov/storage/report.pdf

Vanberg, A. & Ünver, M. (2017). The right to data portability in the GDPR and EU competition law: Odd couple or dynamic duo?. *European Journal of Law and Technology, 8*(1). https://arro.anglia.ac.uk/id/eprint/701565/1/Diker%20Vanberg_2017.pdf