8-24-2020

Cambridge Analytica's Black Box

Margaret Hu

Commentary

BIG DATA & SOCIETY

Big Data & Society
July–December 2020: 1–6

DOI: 10.1177/2053951720938091
journals.sagepub.com/home/bds
SAGE

Cambridge Analytica's black box

Margaret Hu

Abstract

The Cambridge Analytica–Facebook scandal led to widespread concern over the methods deployed by Cambridge Analytica to target voters through psychographic profiling algorithms, built upon Facebook user data. The scandal ultimately led to a record-breaking $5 billion penalty imposed upon Facebook by the Federal Trade Commission (FTC) in July 2019. The FTC action, however, has been criticized as failing to adequately address the privacy and other harms emanating from Facebook's release of approximately 87 million Facebook users' data, which was exploited without user authorization. This Essay summarizes the FTC's response to the Cambridge Analytica–Facebook scandal. It concludes that the scandal focuses attention on the need to explore the potential for embedding due process-type inquiries and protections within the enforcement actions by regulatory agencies such as the FTC. These protections are increasingly important in addressing the problem of "black boxing the voter" that is now presented by data- and algorithmic-driven companies such as Cambridge Analytica and Facebook.

Keywords

Cambridge Analytica, data privacy, due process, Facebook, Federal Trade Commission, voter microtargeting

This article is a part of special theme on The Black Box Society. To see a full list of all articles in this special theme, please click here: https://journals.sagepub.com/page/bds/collections/revisitingtheblackboxsociety

Essay

In Frank Pasquale's seminal work, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Pasquale, 2015), published in 2015, Pasquale observes that algorithms have shifted the gravitational centering of power in modern society. "Deconstructing the black boxes of Big Data isn't easy," explains Pasquale, however: "[i]t matters because authority is increasingly expressed algorithmically" (Pasquale, 2015: 6–8). One year after the publication of Pasquale's book, few could have predicted the manner in which algorithmic tools—combined with the sophisticated "networked nature of modern campaigning" (Hern, 2018)—could potentially manipulate U.S. voters in the 2016 presidential election. The extent to which Black Box (Mayer-Schönberger and Cukier, 2013) algorithms influenced the final outcome of the 2016 presidential election is unknown. What is known, however, is that the Cambridge Analytica -Facebook scandal of 2018 (Berghel, 2018; Hoofnagle, 2018; Isaak and Hanna, 2018; Kang and Confessore, 2018; Kozlowska, 2018; Matz et al., 2017; Persily, 2017; The Wharton School of the University of Pennsylvania, 2018; Ward, 2018) marks how and when the deployment of artificial intelligence (AI) and voter microtargeting (Barocas, 2012; Schipper and Woo, 2017) algorithms arrived in the consciousness of many U.S. voters.

The Cambridge Analytica–Facebook scandal broke on 17 March 2018 (Lapowsky, 2019), when Christopher Wylie stepped forward as a corporate whistleblower and interviewed with the *New York Times* and *The Observer* (Cadwalladr, 2018; Lapowsky, 2019). Wylie, a Canadian data scientist, had served as the former Director of Research for

Penn State Law and School of International Affairs, Institute for Computational and Data Sciences Pennsylvania State University, University Park, PA, USA

Corresponding author:
Margaret Hu, Penn State Law and School of International Affairs, Institute for Computational and Data Sciences Pennsylvania State University, University Park, PA 16802, USA.
Email: Margaret.Hu@psu.edu

Cambridge Analytica and SCL (Strategic Communication Laboratories) Group, the British parent company of Cambridge Analytica. Wylie explained that psychographic profiling enabled Cambridge Analytica to influence voters through the exploitation of social media data to create a "psychological warfare mindf*** tool" (Cadwalladr, 2018; Lapowsky, 2019).

Wylie's disclosure is often referred to as the Cambridge Analytica–Facebook scandal in that his initial testimony eventually led to the revelation that an estimated 87 million Facebook users' data had been harvested by a researcher and then exploited by his company (Kang and Frenkel, 2018). According to media reports, Cambridge Analytica secured the Facebook data from Aleksandr Kogan, a data scientist and psychologist who had been employed as a Lecturer and Senior Research Associate at the University of Cambridge from 2012 to 2018 (University of Cambridge, 2018). Around 2013, Kogan designed a personality profiling app, claiming that the collection of user data was for academic research purposes. Kogan contended that he conformed to Facebook's guidelines at the time (University of Cambridge, 2018).

Kogan's app circulated on Facebook under the title, "thisisyourdigitallife" and the app operated as a personality quiz (Electronic Privacy Information Center, 2019). Users who downloaded the "thisisyourdigitallife" app not only answered questions about themselves, but also granted the app permission to access other parts of their profile, including their "likes," their contact lists, and more (Electronic Privacy Information Center, 2019; Granville, 2018).

In a 2016 news interview, Alexander Nix, the former CEO of Cambridge Analytica, explained that: "we have somewhere close to four or five thousand data points on every individual . . . So we model the personality of every adult across the United States, some 230 million people" (Cheshire, 2016). Later, in June 2018, in testimony before the Digital, Culture, Media, and Sport Committee of the British Parliament, Nix explained that Cambridge Analytica also secured commercial data from data brokers such as Acxiom, Experian, and Infogroup (Lomas, 2018). Through the purchase of privately aggregated databases compiled by U.S. companies on U.S. consumers, Nix revealed that Cambridge Analytica had lawfully acquired millions of data points (Lomas, 2018) on hundreds of millions of U.S. voters. The collected data was then used to fashion Cambridge Analytica's targeting algorithms to predict and influence individual voting behavior in the 2016 presidential election (Electronic Privacy Information Center, 2019; Granville, 2018).

Although much of the Cambridge Analytica–Facebook scandal has focused on Kogan's acquisition of 87 million Facebook users' data, Nix denied that the company relied upon the Kogan data in building its Black Box algorithms. Instead, in the June 2018 testimony before the British Parliament, Nix explained that Cambridge Analytica built its algorithms based on the commercially available data purchased from U.S. companies such as Acxiom, Experian, and Infogroup, combined with publicly and privately available voter data (Lomas, 2018). Siva Vaidhyanathan explains that there is a question as to the extent to which the Trump campaign team relied on Cambridge Analytica data rather than other data: "[W]hen the Trump digital team tried to use Cambridge Analytica data, it found the older, more basic data sets offered by the Republican Party to be more reliable and useful" (Vaidhyanathan, 2019).

In the wake of the Cambridge Analytica–Facebook scandal, the Federal Trade Commission (FTC, 2019a) announced an investigation into the matter (Cambridge Analytica Complaint and Facebook Complaint). As many experts recognize, this agency plays an outsized role in upholding data privacy protections in the United States (Bamberger and Mulligan, 2011; Barrett, 2019; Hartzog, 2015; Hoofnagle, 2016; Pasquale, 2012; Solove and Hartzog, 2014). Yet, the FTC is unable to address many of the most serious concerns raised by the Cambridge Analytica–Facebook scandal. The FTC's Section 5 authority under the FTC Act is limited to addressing "unfair or deceptive acts or practices in or affecting commerce" (*Facebook* Complaint, 2011; *Federal Trade Act 1914*, 15 U.S.C. § 45 *et seq*., 2018). The manner in which the FTC resolved the Cambridge Analytica–Facebook scandal helped to reveal the uncomfortable limitations of the FTC's enforcement authority.

The FTC launched an investigation into Facebook's consumer data privacy policies and practices in March 2018 (Romm and Timburg, 2018). The investigation sought to uncover whether Facebook had violated a privacy consent agreement it had entered into with the FTC in 2011 to protect consumers against the unauthorized disclosure of private user data to third parties (Granville, 2018). In 2019, Facebook settled with the FTC (Kang, 2019). The settlement, announced on 24 July 2019, included a record-setting $5 billion fine and an FTC Order to institute new privacy standards (Kang, 2019).

As per the FTC Order, for Facebook to disclose private user information to third parties engaged in commerce, Facebook must now obtain a user's express consent in conjunction with disclosing to the user the third party's identity, the categories of nonpublic information disclosed, and that the sharing of such goes beyond the privacy settings the user has specified (United States v. Facebook Inc., 2019). Furthermore, Facebook must restrict third-party access to specified

user information within 30 days if the user has deleted information or terminated his or her account. However, this rule does not apply to situations where a separate person has shared the user's deleted information with their own account. Within 120 days of a user deleting specified user information or terminating their account, with few exceptions, Facebook must also delete the information, or make it unidentifiable, on Facebook's own servers (United States v. Facebook Inc., 2019).

Other new privacy regulations instituted by the Order require Facebook to prohibit third-party applications or websites from requiring or requesting a user to input their Facebook password to gain access to the third-party product; to cryptographically protect user passwords when transmitted over the Internet; and to delete, cryptographically protect, or render unidentifiable any user passwords stored in Facebook's data warehouse (United States v. Facebook Inc., 2019). As to facial recognition technology, Facebook must obtain a user's express consent to use of facial recognition technology—separate from other data privacy consent obtained by the company—and must notify the user how facial recognition will be used and who it will be shared with, before Facebook can share the facial recognition data with third parties engaged in any commerce (United States v. Facebook Inc., 2019). If these requirements are not satisfied, Facebook has been ordered to delete any facial recognition templates it has stored in connection to third parties engaged in any commercial activity (United States v. Facebook Inc., 2019).

Immediately after the FTC announced the terms of the 2019 settlement, including the $5 billion penalty that was assessed against Facebook as a result of the FTC's investigation into the Cambridge Analytica–Facebook scandal, privacy experts expressed concern about the efficacy and rigor of the agency's enforcement actions. In his dissent to the 2019 settlement agreement, FTC Commissioner Rohit Chopra expresses deep reservations over the settlement, stating that while the FTC managed to generate headlines through the assessment of a $5 billion penalty, the settlement was inadequate to address Facebook's behavior (*Facebook* Chopra Dissent, 2019c). Chopra also implicitly invites an inquiry into how the $5 billion penalty was calculated. In his dissent, he notes that in the FTC's settlement with Google, the FTC calculated the company's unjust gains and then assessed a penalty that was "more than five times the company's unjust gains" (*Facebook* Chopra Dissent, 2019c). Here, Chopra observes that not only did the FTC fail to seek higher penalties, even though higher penalties may have been available, the FTC also failed to "cite to any analysis of Facebook's unjust enrichment" from the violation (*Facebook* Chopra Dissent, 2019c).

Chopra was not the only dissenting voice to speak out against the FTC's response. FTC Commissioner Rebecca Slaughter opined that in order to ensure greater transparency in understanding the nature of the violation, and greater transparency in fashioning the remedy, proceeding to litigation may have been more appropriate. Commissioner Slaughter explained in her dissenting statement that she declined to join the settlement and instead believed that the FTC "should have initiated litigation against Facebook and its CEO Mark Zuckerberg. The Commission would better serve the public interest and be more likely to effectively change Facebook by fighting for the right outcome in a public court of law" (*Facebook* Slaughter Dissent, 2019b).

Even before the announcement of the $5 billion fine, David Vladeck, former Director of FTC's Bureau of Consumer Protection, had predicted that the FTC would be "unlikely to investigate the most troubling aspects of the Cambridge Analytica matter – namely, the harvesting of user-specific data which was then deployed to shape that user's political views, all done to influence the election" (Vladeck, 2018). He pointed out that this was "[b]ecause of [the FTC's] limited statutory authorization and the constraints of the First Amendment" (Vladeck, 2018). Important scholarship on the First Amendment implications of social media and platform regulation go beyond the scope of this Essay (Bambauer, 2016; Klonick, 2018; Richards, 2013, 2015). The Cambridge Analytica–Facebook scandal brings into sharp relief a disconcerting question: what due process protections might be available for algorithmic-based harms that are introduced by private corporations and, consequently, fall outside of constitutional due process protections. According to Vladeck: "[t]here should be little doubt that Facebook user data sharpened Cambridge Analytica's algorithms, which made the Trump campaign's micro-targeted messaging more effective" (Vladeck, 2018).

Moving forward, experts have proposed a response to the Cambridge Analytica–Facebook scandal that draws upon multiple reforms in law and policy. Some proposals focus on increasing the effectiveness of the FTC and include providing the FTC with more resources, such as increased funding and the ability to hire and retain in-house experts (Barrett, 2019; Hoofnagle et al., 2019); granting the agency more explicit statutory authority (Maass, 2012; Pasquale, 2012; Vladeck, 2018), such as more clearly defining privacy harms and abuses that might fall within FTC's enforcement (Hartzog, 2015; Hoofnagle, 2016; Solove and Hartzog, 2014); and clarifying other ambiguities in consumer privacy law (FTC Hearing, 2018). Some look to a

future that includes FTC promotion of corporate adopted policies that embrace privacy and security-by-design principles (Hartzog, 2018; McSweeny, 2018), and, relatedly, FTC promotion of self-regulatory reforms that consider data ethics and digital ethics in day-to-day corporate and product-service governance (Hartzog, 2018; McSweeny, 2018). In increasing the effectiveness of general privacy law, experts also champion increasing consumer data controls, such as data portability (Cicilline and McSweeny, 2018); expanding antitrust law to increase competition and better serve consumers (Cicilline and McSweeny, 2018; Khan, 2016; Pasquale, 2013); tort law reform and, for example, one scholar's proposal to hold companies such as Facebook accountable as information fiduciaries (e.g. duty of care, duty of loyalty, duty of confidentiality) (Balkin, 2018); and looking to omnibus privacy law reforms, such as the adoption of more comprehensive legal frameworks (Hoofnagle et al., 2019) that can more directly target the regulation of algorithmic decision-making.

The Cambridge Analytica–Facebook scandal also sheds light on the possibility of embedding stronger due process-type inquiries, including both procedural and substantive due process, into FTC's security and privacy enforcement actions. In recent years, multiple scholars have proposed due process protections to guard against Big Data- and algorithmic-based harms (Citron, 2008; Citron and Pasquale, 2014; Crawford and Schultz, 2014; Hu, 2016). Other scholars have called for a more careful academic and legal critique of Big Data's impact (Barocas and Selbst, 2016; Boyd and Crawford, 2012; Eubanks, 2018; Hu, 2016; Mayer-Schönberger and Cukier, 2013; O'Neil, 2016; Richards and King, 2014; Tene and Polonetsky, 2012). Danielle Keats Citron's seminal work on technological due process appears to be an influencing force on the FTC's Order (Citron, 2008). Although constitutional due process protections extend to government actions and not private actions, in prior scholarship, Citron and Pasquale presciently raised the question of what heightened role the FTC could play in protecting against classification-based harms posed by an increasingly algorithmically "scored society" (Citron and Pasquale, 2014).

Because Cambridge Analytica's psychographic profiling of U.S. voters poses a threat to the electoral process, the practice should be contextualized as a black box challenge to democratic institutions broadly. The FTC's Order imposes significant regulatory obligations on Facebook moving forward and more robustly attempts to protect the data privacy interests of consumers (*Facebook* Slaughter Dissent, 2019b). The FTC Order does not safeguard the fundamental constitutional rights that are at risk to U.S. voters through the deployment of AI and algorithms that aim to disrupt voters' core freedoms surrounding individual autonomy and dignity rights. Due process-type inquiries and protections could be embedded within regulatory agencies such as the enforcement actions of the FTC. The protective actions proposed by Citron and Pasquale and other experts—such as increasing access to data sets, requiring greater transparency in algorithms, and requiring algorithmic testing for impact—are increasingly important. In order to properly address the problem of "black boxing the voter" that is now presented by data- and algorithmic-driven companies such as Cambridge Analytica and Facebook, a more searching inquiry into reform is pressing. Future developments in law and policy must now evolve to encompass newly emerging harms posed by black boxing the voter.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

ORCID iD

Margaret Hu https://orcid.org/0000-0002-9844-1773

References

Balkin J (2018) Free speech is a triangle. *Columbia Law Review* 118: 2051–2052. Available at: https://columbialawreview.org/content/free-speech-is-a-triangle/ (accessed 25 October 2019).

Bambauer J (2016) The relationships between speech and conduct. *U.C. Davis Law Review* 49:1949–1953. Available at: https://lawreview.law.ucdavis.edu/issues/49/5/Response/49-5_Bambauer.pdf (accessed 25 October 2018).

Bamberger K and Mulligan D (2011) Privacy on the books and on the ground. *Stanford Law Review* 63: 273–275, 279, 283–285. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1568385 (accessed 25 October 2019).

Barocas S (2012) The price of precision: Voter microtargeting and its potential harms to the democratic process. In: *Proceedings of the first edition workshop on politics, elections and data*. CIKM'12: 21st ACM (Association for Computing Machinery) international conference on information and knowledge management, 1-2 November 2012, pp.31–36. US: Association for Computing Machinery. Available at: http://delivery.acm.org/10.1145/2390000/2389671/p31barocas.pdf?ip=137.113.127.19&id=2389671&acc=ACTIVE%20SERVICE&key=B3324

0AC40EC9E30% 2E6792A2BEFAB43BD2%2E4D4702B0C3E38B35%
2E4D4702B0C3E38B35&__acm__=1565830487_9ec3a56782ebd97240c67932a5f5f88f (accessed 25 October 2019).

Barocas S and Selbst A (2016) Big Data's disparate impact. *California Law Review* 104: 671.

Barrett L (2019) Confiding in Con Men: U.S. Privacy law, the GDPR, and information fiduciaries. *Seattle University Law Review* 42: 1075.

Berghel H (2018) Malice domestic: The Cambridge Analytica dystopia. *Computer* 51: 84–89.

Boyd D and Crawford K (2012) Critical questions for Big Data: Provocations for a cultural, technological, and scholarly phenomenon. *Information, Communication & Society* 15: 662–679.

Cadwalladr C (2018) 'I made Steve Bannon's psychological warfare tool': Meet the data war whistleblower. *The Observer*, 18 March.

Cheshire T (2016) Behind the scenes at Donald Trump's UK digital war room. *Sky News*, 21 October.

Cicilline D and McSweeny T (2018) Competition is at the heart of Facebook's privacy problem. *Wired*, 24 April. Available at: https://www.wired.com/story/competition-is-at-the-heart-of-facebooks-privacy-problem/ (accessed 25 October 2019).

Citron D (2008) Technological due process. *Washington University Law Review* 85: 1249.

Citron D and Pasquale F (2014) The scored society: Due process for automated predictions. *Washington Law Review* 89: 3–4.

Crawford K and Schultz J (2014) Big Data and due process: Toward a framework to redress predictive privacy harms. *Boston College Law Review* 55: 96.

Electronic Privacy Information Center (2019) In re Facebook – Cambridge Analytica. Available at: https://epic.org/privacy/facebook/cambridge-analytica/ (accessed 25 October 2019).

Eubanks V (2018) *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. New York: St. Martin's Press.

Federal Trade Act 1914, 15 U.S.C. § 45 *et seq*. (2018).

Federal Trade Commission (2011) *In the Matter of Facebook, Inc*. Complaint. Available at: https://www.ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookcmpt.pdf (accessed 25 October 2019).

Federal Trade Commission (2018) *Competition and Consumer Protection in the 21st Century: Hearing Before the Fed. Trade Comm'n*. Available at: https://www.ftc.gov/system/files/documents/public_statements/1408196/chopra_-_comment_to_hearing_1_9-6-18.pdf (accessed 5 August 2020).

Federal Trade Commission (2019a) *In the Matter of Cambridge Analytica, LLC, a Corporation,* Complaint Docket No. 9383. Available at: https://www.ftc.gov/system/files/documents/cases/182_3107_cambridge_analytica_administrative_complaint_7-24-19.pdf (accessed 25 October 2019).

Federal Trade Commission (2019b) *In the Matter of Facebook, Inc*. Dissenting Statement of [FTC] Commissioner Rebecca Slaughter, Docket No. 1823109. Available at: https://www.ftc.gov/system/files/documents/public_statements/1536918/182_3109_slaughter_statement_on_facebook_7-24-19.pdf (accessed 25 October 2019).

Federal Trade Commission (2019c) *In the Matter of Facebook, Inc*. Dissenting Statement of [FTC] Commissioner Rohit Chopra, Docket No. 1823109. Available at: https://www.ftc.gov/system/files/documents/public_statements/1536911/chopra_dissenting_statement_on_facebook_7-24-19.pdf (accessed 25 October 2019).

Granville K (2018) Facebook and Cambridge Analytica: What you need to know as fallout widens. *The New York Times*, 19 March.

Hartzog W (2015) The scope and potential of FTC data protection. *George Washington Law Review* 83: 2230.

Hartzog W (2018) *Privacy's Blueprint: The Battle to Control the Design of New Technologies*. Cambridge: Harvard University Press.

Hern A (2018) Cambridge Analytica: How did it turn clicks into votes? *The Guardian*, 6 May.

Hoofnagle C (2016) Federal Trade Commission Privacy Law and Policy. New York: Cambridge University Press.

Hoofnagle C (2018) Facebook in the Spotlight: Dataism vs. Privacy. *Jurist*, 20 April. Available at: https://www.jurist.org/commentary/2018/04/chris-hoofnagle-facebook-dataism/ (accessed 25 October 2019).

Hoofnagle C, Hartzog W and Solove D (2019) The FTC can rise to the privacy challenge, but not without help from Congress. *Brookings Institution*, 8 August. Available at: https://www.brookings.edu/blog/techtank/2019/08/08/the-ftc-can-rise-to-the-privacy-challenge-but-not-without-help-from-congress/ (accessed 20 November 2019).

Hu M (2016) Big Data blacklisting. *Florida Law Review* 67: 1735.

Isaak J and Hanna M (2018) User data privacy: Facebook, Cambridge Analytica, and privacy protection. *Institute of Electrical and Electronics Engineers* 51: 56–59.

Kang C (2019) F.T.C. approves Facebook fine of about $5 billion. *The New York Times*, 12 July.

Kang C and Confessore N (2018) Facebook data scandals stoke criticism that a privacy watchdog too rarely bites. *The New York Times*, 30 December. Available at: https://www.nytimes.com/2018/12/30/technology/facebook-data-privacy-ftc.html?rref=collection%2Fbyline%2Fcecilia-kang&action=click&contentCollection=undefined&region=stream&module=stream_unit&version=latest&contentPlacement=1&pgtype=collection (accessed 25 October 2019).

Kang C and Frenkel S (2018) Facebook says Cambridge Analytica harvested data of up to 87 million users. *The New York Times*, 14 April.

Khan L (2016) Amazon's antitrust paradox. *Yale Law Journal* 126: 710. Available at: https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=5785&context=ylj

Klonick K (2018) The new governors: The people, rules, and processes governing online speech. *Harvard Law Review* 131: 1598. Available at: https://harvardlawreview.org/2018/04/the-new-governors-the-people-rules-and-processes-governing-online-speech/ (accessed 25 October 2019).

Kozlowska I (2018) Facebook and data privacy in the age of Cambridge Analytica. *Henry M. Jackson School of International Studies, University of Washington*, 30 April. Available at: https://jsis.washington.edu/news/facebook-data-privacy-age-cambridge-analytica/ (accessed 25 October 2019).

Lapowsky I (2019) How Cambridge Analytica sparked the great privacy awakening. *Wired*, 17 March.

Lomas N (2018) Cambridge Analytica's Nix said it licensed 'millions of data points' from Acxiom, Experian, InfoGroup to target US voters. *Tech Crunch*, 6 June.

Maass P (2012) Your FTC privacy watchdogs: Low-tech, defensive, toothless. *Wired*, 28 June. Available at: https://www.wired.com/2012/06/ftc-fail/ (accessed 24 October 2019).

Matz SC, Kosinski M, Nave G, et al. (2017) Psychological targeting as an effective approach to digital mass persuasion. *Proceedings of the National Academy of Sciences of the United States of America* 114: 12714–12719.

Mayer-Schönberger V and Cukier K (2013) *Big Data: A Revolution That Will Transform How We Live, Work, and Think*. London: Hodder and Stoughton.

McSweeny T (2018) Psychographics, predictive analytics, artificial intelligence & bots: Is the FTC keeping pace? *Georgia Law and Technology Review* 2: 529.

O'Neil C (2016) *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. New York: Crown.

Pasquale F (2012) FTC Agonistes: From the Nader Report to the Wired Report. *Balkinization*. Available at: https://balkin.blogspot.com/2012/08/ftc-agonistes-from-nader-report-to.html (accessed 24 October 2019).

Pasquale F (2013) Privacy, antitrust, and power. *George Mason Law Review* 20: 1009. Available at: https://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?article=2347&context=fac_pubs (accessed 20 November 2019).

Pasquale F (2015) *The Black Box Society: The Secret Algorithms that Control Money and Information*. Cambridge: Harvard University Press.

Persily N (2017) The 2016 U.S. election: Can democracy survive the Internet? *Journal of Democracy* 28: 63–76.

Richards N (2013) The dangers of surveillance. *Harvard Law Review* 126: 1934. Available at: https://harvardlawreview.org/wp-content/uploads/pdfs/vol126_richards.pdf

Richards N (2015) *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age*. Oxford: Oxford University Press.

Richards N and King J (2014) Big Data ethics. *Wake Forest Law Review* 49: 393. Available at: https://ssrn.com/abstract=2384174

Romm T and Timburg C (2018) FTC opens investigation into Facebook after Cambridge Analytica scrapes millions of users' personal information. *The Washington Post*, 20 March.

Schipper B and Woo HY (2017) Political awareness, microtargeting of voters, and negative electoral campaigning. *University of California, Davis*, 2 May. Available at: https://pdfs.semanticscholar.org/21c8/566614892daecf4738c29b907d976126d49b.pdf (accessed 25 October 2019).

Solove D and Hartzog W (2014) The FTC and the New Common Law of Privacy. *Columbia Law Review* 114: 583.

Tene O and Polonetsky J (2012) Privacy in the age of Big Data: A time for big decisions. *Stanford Law Review Online* 64: 63.

The Wharton School of the University of Pennsylvania (2018) Why the Cambridge Analytica Scandal is a watershed moment for social media. Available at: https://knowledge.wharton.upenn.edu/article/fallout-cambridge-analytica/ (accessed 25 October 2019).

United States v. Facebook, Inc. (D.C. 24 July 2019) Stipulated Order for Civil Penalty, Monetary Judgment, and Injunctive Relief No. 19-cv-2184. Available at: https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_order_filed_7-24-19.pdf (accessed 5 August 2020).

University of Cambridge (2018) Statement by the University of Cambridge about Dr. Aleksandr Kogan. Available at: https://www.cam.ac.uk/notices/news/statement-from-the-university-of-cambridge-about-dr-aleksandr-kogan (accessed 25 October 2019).

Vaidhyanathan S (2019) *Antisocial Media: How Facebook Disconnects Us and Undermines Democracy*. New York: Oxford University Press, pp.155–156.

Vladeck D (2018) Facebook, Cambridge Analytica, and the regulator's dilemma: Clueless or Venal? *Harvard Law Review Blog*. Available at: https://blog.harvardlawreview.org/facebook-cambridge-analytica-and-the-regulators-dilemma-clueless-or-venal/ (accessed 25 October 2019).

Ward K (2018) Social networks, the 2016 US presidential election, and Kantian ethics: Applying the categorical imperative to Cambridge Analytica's behavioral microtargeting. *Journal of Media Ethics* 33: 133–148.