Surveillance & Society

Article

Defunding Hate: PayPal's Regulation of Hate Groups

Natasha Tusikov

York University, Canada
ntusikov@yorku.ca

Abstract

The riot by white supremacists in Charlottesville, Virginia, in August 2017, generated a public debate about the role of platforms in policing users involved in violent hate speech. PayPal's efforts on this issue, in removing services from some designated hate groups while continuing to serve others, highlights the challenges payment platforms face when they act, whether formally or informally, as regulators. This article examines PayPal's policies and enforcement efforts, both proactive and reactive, in removing its services from hate groups in the United States. It pays particular attention to the surveillance and screening practices that PayPal employs to proactively detect users who violate its policies. The article argues that public calls for PayPal to identify and remove its services from hate groups raise critical questions about ceding broad regulatory authority to platforms and reveal the serious challenges of relying upon commercial enterprises to address complex social problems.

Introduction

The torch-lit march by armed white supremacists in Charlottesville, Virginia, in August 2017, ignited a public debate about the role of internet companies in policing their platforms to remove hate groups.[1] Following mounting public pressure and media coverage of the violence that took place during that march, multiple US-based internet companies, including Google, PayPal, and the domain registrar GoDaddy, terminated their services to white supremacist websites and platforms, such as the social network Gab, which has about 400,000 users, mostly in the United States, United Kingdom, Australia, Canada, and Germany (GAB AI Inc. 2018: 1). Launched in 2016, Gab was created to be a friendly space for those who "share the common ideals of Western values, individual liberty, and the free exchange and flow of information" (GAB AI Inc. 2018: 5) and has become the "alt right" platform of choice for white supremacists. Platforms' provision of critical commercial and technical services like payment processing was again in the public spotlight, following the killing of eleven people at the Tree of Life synagogue in Pittsburgh in October 2018. The man charged in the shooting had posted anti-Semitic messages to Gab just prior to the attack (Amend 2018). Following the synagogue shooting, internet companies, including PayPal, removed their services from Gab.

[1] "Hate speech" varies among legal jurisdictions. This article adopts the definition of hate group from the Southern Poverty Law Centre, an anti-hate legal-advocacy organization, as that which "based on its official statements or principles, the statements of its leaders, or its activities—has beliefs or practices that attack or malign an entire class of people, typically for their immutable characteristics" (Southern Poverty Law Centre n.d.).

Tusikov, Natasha. 2019. Defunding Hate: PayPal's Regulation of Hate Groups. *Surveillance & Society* 17(1/2): 46-53.
https://ojs.library.queensu.ca/index.php/surveillance-and-society/index | ISSN: 1477-7487

The incidents in Charlottesville and Pittsburgh starkly highlight the pressure internet platforms face in policing hate groups. "Platforms" here refers to entities, often from the private sector, which provide or facilitate internet services, such as payment, search, social networking, advertising, web hosting, or domain names. Platforms' responsibility for removing certain types of third-party content stretches back to the early 1990s (see Zittrain 2006), and such responsibility can stem from statutory requirements or take the form of informal industry regulation (see Laidlaw 2012; Tusikov 2016).

This article argues that PayPal has a considerable regulatory capacity that stems from two fundamental features of platforms. First, platforms grant themselves considerable latitude, through their contractual terms-of-use agreements with their users, to interpret and enforce their rules, such as those concerning the promotion of hate. Platforms' implementation and enforcement of these rules, typically undertaken with little independent oversight or public disclosure (see Tusikov 2016), constitute a form of private ordering (Schwarcz 2002). Dominant platforms like PayPal can institute their rules over hundreds of millions of people. Second, PayPal's regulatory capacity relies on its routine surveillance of its users' activities and transactions as part of its data-intensive business model that is characteristic of surveillance capitalism (Zuboff 2015). The platform not only employs surveillance to police its users for violations of its policies but also, more importantly, to collect and interpret data on its users in order to serve its commercial interests. More broadly, platforms' recent role in policing hate groups highlights the serious problems of ceding regulatory authority to platforms to address complex social problems.

The rest of the article is organized into four parts. The first describes PayPal's operations and then explains how the platform regulates through surveillance. Next, the article examines PayPal's recent efforts to police hate groups in the United States before moving to explain why platforms respond reactively to hate groups. Finally, the article highlights the challenges of platforms' defunding of hate groups. A brief conclusion follows.

PayPal as a Regulator

Much scholarly attention focuses on efforts by social media platforms, like Twitter and Facebook, to remove content that promotes hate and to expel egregious offenders (see Gillespie 2018). Payment providers, in contrast, have elicited little scholarly attention (notable exceptions include Bridy 2015; Tusikov 2016). Being expelled from social media platforms has the potential to silence or subdue targeted individuals, although they may move to other platforms like Gab. Payment platforms, however, have the capacity to strangle revenue flows by removing individuals' capacity to raise donations or sell goods (see Mann and Belzley 2005; McCoy et al. 2012). Despite the growing number of payment methods, the online payment industry remains highly concentrated. Once the largest payment providers—Visa, MasterCard, and PayPal—terminate their services, users may struggle to find reliable, commercially viable alternatives (see McCoy et al. 2012). Payment platforms can therefore effectively defund targeted entities and terminate commercial activities.

Created in 1998, PayPal is an online payment company that performs money transfers and processes payments. In 2017, it had 229 million active accounts and processed more than 7.8 billion payment transactions valued at more than USD $456 billion (PayPal 2018: 5). Like all platforms, PayPal sets out rules that incorporate national laws, such as those that prohibit fraud, and also industry- or company-specific rules within a series of legal agreements it enters into with its users. It its acceptable user policy, PayPal prohibits the use of its services for transactions involving "the promotion of hate, violence, racial or other forms of intolerance that is discriminatory" (PayPal 2015). If users violate its rules, PayPal "may close, suspend, or limit your access to your Account or the PayPal Services, and/or limit access to your funds" (PayPal 2018a).

PayPal enables its users to make payments from a PayPal account, bank account, or through debit or credit cards. In order to allow its customers to use credit/debit cards, PayPal must abide by rules set by payment card networks (e.g., Visa and MasterCard), as must PayPal's users. Commercial entities, termed

"merchants" that want to offer PayPal as a payment option, must comply not only with PayPal's rules but also with those of the payment card companies and banks that issue credit cards. Each merchant that offers PayPal as one of its payment methods must comply with PayPal's commercial entity agreement, a legally binding contract that sets out the rules under which the merchant can accept payment through payment cards (see PayPal 2018a). Simply put, merchants that offer customers the option to pay through PayPal, on their websites, must comply with all of PayPal's rules, as well as those rules set out and interpreted by payment card networks.[2]

Regulation through Surveillance

PayPal's defunding of specific US-based hate groups is a form of private ordering (Schwarcz 2002) in which platforms have a quasi-legislative power to set and enforce rules over their users and a quasi-executive power to enforce those rules through technical means (Belli and Venturini 2016: 4; see also Langenderfer 2009). Specifically, platforms can designate certain behavior as "inappropriate" for their services, even if that behavior is lawful and, in the absence of formal legal orders, issue user sanctions such as temporary or permanent suspension. While the Charlottesville and Pittsburgh incidents highlighted platforms' efforts to police hate groups, private actors' adoption of increased regulatory duties during periods of technological innovation is not unusual (see e.g., Cafaggi 2012; Zittrain 2006). New technologies can redistribute regulatory capacity to private actors or augment an existing capacity for governance, particularly if governments are perceived as ill equipped, unable, or unwilling to act (see Cafaggi 2012). PayPal is not new to policing its platform: it removes its payment services from actors involved in copyright infringement (Bridy 2015), child pornography (Laidlaw 2012), and those selling counterfeit goods (Lindenbaum and Ewen 2012; Tusikov 2016).

Platforms' regulatory capacity and their systems of private ordering are inextricably tied to their business models; these models rely on the mass accumulation and the interpretation of users' personal data in a practice that is characteristic of surveillance capitalism (Zuboff 2015). The aim of surveillance capitalism is to influence and predict consumer behavior through mass, often automated data collection and data analytics in order to generate revenue and exert market control within industry sectors (Zuboff 2015: 75; see also West 2019).

While PayPal may not be commonly understood as having a surveillance capitalist business model, the platform undertakes data-driven practices to identify patterns and anticipate trends for commercial purposes and for security-oriented surveillance. PayPal employs both reactive and proactive surveillance practices: the latter enables the platform to intervene pre-emptively to remove bad actors (see Lyon 2014), before the platform receives complaints or negative media coverage. These surveillance practices entail a system of dataveillance (Van Dijck 2014) in which monitoring practices are deliberately broadened from focused attention on targeted individuals (see Lyon 2014), to a system of pervasive continuous monitoring. Dataveillance is thus an intrinsic feature of surveillance capitalism, as the latter's goal is to enable platforms' commercial imperative of discerning patterns in data to understand and, more importantly, predict consumer behavior (see Zuboff 2015).

PayPal's dataveillance practices are evident in its intensive monitoring of its users and their transactions. Depending on how its services are used, PayPal collects personal data, such as the fund sender's name, mailing and email addresses, telephone numbers and account numbers, as well as information on the party receiving the funds (PayPal 2018b). PayPal also collects data on transaction amounts, merchant information, and location, as well as information on the devices used to access PayPal, such as network connections, IP addresses, web browsers, information on apps used on the devices, and biometric data (e.g., fingerprints used to verify the users' identities) (PayPal 2018b). Payment platforms' data can reveal highly sensitive information about people's political views, religion, health, and sexual habits.

[2] Visa and MasterCard do not have specific rules that prohibit the promotion of hate, but both prohibit any illegal activities (see e.g., Sec. 1.5.2 of Visa 2018). Following the Charlottesville case, both companies removed their services from groups that they contended engaged in illegal activity, such as inciting violence (Koren 2017).

In a classic example of surveillance capitalism, PayPal collects data on its customers' social media use, if its customers grant permission. PayPal allows users to connect their PayPal account to social media platforms, like Twitter or Facebook, which PayPal terms a "significant benefit and innovation of PayPal's Services" (PayPal 2018b). When people link their PayPal and social media accounts, the companies "exchange your Personal Data and other information directly" (PayPal 2018b), thereby considerably enhancing PayPal's capacity to gather detailed personal data on its customers, including their social contacts, activities, attitudes, and interests. In doing so, platforms can fulfill the surveillance capitalist logic of anticipating future products and services. PayPal's interest in mining social media data is also evident in its ownership of Venmo, a mobile payment application with a social networking function that enables users to share messages and details of their financial transactions with their friends. Created in 2009, Venmo was designed to help people split restaurant bills or taxi fare among friends, hence the social media application of this payment service. Venmo collects detailed information from its users, specifically data from users' social networks, like Twitter and Facebook, and email service providers, and then shares this information with PayPal (Venmo 2018).

PayPal's entry into social media data collection and Venmo's distinctive blending of financial and social media services illustrate how important it is for platforms to accord to ever wider and more pervasive data accumulation and analysis. In particular, PayPal's efforts in this area exemplify platforms' practice of datafication in which platforms collect, interpret, and commodify data in order to augment existing products and services and create new ones (Mayer-Schönberger and Cukier 2013; Van Dijck 2014; Zuboff 2015). The intention is to transform data into "surveillance assets" (Zuboff 2015: 81) so that platforms can extract new patterns and understandings of users' behavior. Platforms' data-driven business models and cultivation of surveillance assets result in power asymmetries that favor actors with the access, capabilities, and technical prowess to interpret data (West 2019: 20; see also Zuboff 2015). Given platforms' data-intensive business practices, they would appear well positioned to identify problematic actors who use their services, especially those in repeated breach of their policies.

Defunding Hate

PayPal employs "proactive monitoring, screening and scrutiny" to identify problems and a "highly trained team of experts [that] addresses each case individually," explained senior PayPal executive in a written statement following the violence in Charlottesville (Paasche 2017). Despite platforms' carefully articulated policies and surveillance-intensive enforcement practices, however, their enforcement efforts against hate groups are often reactive and arbitrary. "It took blood in the streets for the tech industry to finally face its domestic extremism problem" (Amend 2018a), argued the Southern Poverty Law Centre (SPLC), a prominent US anti-hate legal advocacy organization that identifies and tracks hate groups. Two US advocacy groups, Color of Change and the SPLC, are pressuring platforms, including Facebook, Twitter, Google, and PayPal, to take a more comprehensive, proactive approach against organizations involved in violent hate speech. Directly after the white supremacist march in Charlottesville, for example, the SPLC released a report documenting the white supremacist groups and individuals that were raising money using PayPal (see Hatewatch 2017).

PayPal has responded to pressure from these groups, as have other platforms. After the Charlottesville violence, PayPal pulled its services from 34 organizations the SPLC identified as hate groups (Jan 2017; Hatewatch 2017). After the Pittsburgh shooting, PayPal also withdrew its services from Gab, saying it had been "closely monitoring" Gab and was "in the process of canceling the site's account before today's tragic events occurred" (CNet 2018). Other platforms, however, have taken more rapid action than PayPal. Google Play kicked Gab off its platform in August 2017, in the wake of the Charlottesville violence, for violating its policies on promoting hatred and violence (Lee 2017). It was fourteen months later—in the wake of the Pittsburgh shootings—that PayPal also banned Gab. What's more, PayPal's regulatory efforts seem arbitrary, with the removal of services from some individuals and groups the SPLC identifies as involved in hate speech, but not others. In 2015, for example, two months after PayPal requested from the SPLC a

list of far-right groups that were raising money through PayPal, the provider was still processing payments for some of the targeted groups (Hankes 2015).

This analysis of PayPal is based on publicly reported cases covered in the media or by civil society groups. In PayPal's defence, the platform may be proactively—and quietly—removing its services from individuals and organizations. However, this does not explain why it continues to provide payment services to some actors the SPLC judges to be the most active and prominent hate groups in the United States. Moreover, advocacy groups are rightfully concerned about the length of some of its investigations. Gab, for instance, has openly promoted violently racist, anti-Semitic, and discriminatory speech since it was created in 2016 (see Glaser 2017). Yet it took over a year for PayPal to terminate its services to Gab, which raises serious questions about the effectiveness of PayPal's enforcement practices as well as the platform's commitment to addressing the promotion of hate.

Platforms' Reactive Response

The Charlottesville and Pittsburgh cases demonstrate platforms' tendency to govern in response to specific crises, media coverage, or public or political pressure. Platforms' reactive responses highlight a larger problem of failing to remove users that are in clear—and in some cases, publicly defiant—violation of their anti-hate policies. Simply put, platforms are failing to remove users for promoting violent hate speech.

One explanation for PayPal's sometimes sluggish response to dealing with hate groups is that identifying wrongdoing can be difficult, particularly for platforms with millions of users and billions of transactions. In contrast to child sexual abuse images, it can be challenging to identify, with precision, content that "promotes" hate or violence. While it may be immediately apparent that certain content is distasteful or vile, platforms may have a more difficult time distinguishing that which promotes hate or violence. PayPal's Dan Schulman, chief executive officer, argues, "the difference between free speech and hatred is a difficult line to cross" (Bond 2018). Such challenges do not fully explain platforms' largely passive response to hate groups, as platforms have the latitude to interpret their policies as broadly or narrowly as they wish. They grant themselves the right to withdraw services from users at any time and for any reason, without advance notice to users and without liability to the platform (see PayPal 2018a).

PayPal's defunding of hate groups invites scrutiny of the platform's commercial surveillance practices. Platforms have commercial imperatives that may conflict with their regulatory efforts. Platforms may act in response to negative media coverage or civil society lobbying in order to protect their corporate reputations, but may also fear angering users who interpret such actions as censorship. Fundamentally, surveillance capitalism emphasizes the pervasive accumulation of data, which is oriented toward acquiring ever more users and data, even when such practices may cause harm to other users, as has been the case with social media platforms (see Gillespie 2018).

Platforms' socio-political and legal environments also shape their regulatory practices. Hateful speech and its regulation are context dependent (see e.g., Tenove et al. 2018). US-based platforms typically express a strong ideological support for free speech that reflects US constitutional values. This cultural value shapes US platforms' regulatory practices, influencing the lawyers who craft and enforce their rules (see e.g., Klonick 2018). PayPal's executives explain that the platform "work[s] hard to achieve the right balance" between free expression and "the principles of tolerance, diversity and respect" (PayPal 2018c). The United States legally permits hate speech that, for example, could constitute violations of criminal law in Canada or Germany (see Tenove et al. 2018). US-based platforms' reactive response to hate groups can, in part, be understood as their lack of a legal obligation to act against hate groups in the United States and, more importantly, their strong support for free speech.

Consequences

Ceding regulatory authority to commercial actors to target hate groups, whether proactively or reactively, raises serious procedural and normative challenges. First, such regulation often occurs in the absence of due

process. Actors may not be informed before they lose critical commercial services or meaningful explanations may be absent, and platforms may lack robust appeals processes. Further, platforms' regulatory efforts are troublingly arbitrary with only some actors targeted. Platforms' use of automation to identify or act against suspected wrongdoers may also magnify problems of due process.

Second, commercial entities are acting as arbiters of lawful speech but typically with little accountability. Many may support PayPal's removal of its services from Gab, but other cases are less straightforward. A growing body of scholarship shows private actors' policing of speech disproportionately affects marginalized or vulnerable actors engaging in controversial or critical speech but not violent speech, such as Black Lives Matter protesters (see e.g., Noble 2018).

Third, platforms' regulatory practices regarding hate groups are troublingly opaque, although some practices are more transparent than others. Facebook and Google publish some statistics regarding the removal of hateful content (see e.g., Facebook 2018), but PayPal does not publicly explain why it terminates services to some actors but not others, or why it may take longer than other platforms to ban hate groups. Platforms need to be more transparent about their regulatory practices and enforcement results, a principle that digital rights organizations have long advocated (see, e.g., McSherry et al. 2018). Publishing transparency reports that detail enforcement efforts are a good first step, although such reports are not sufficient in themselves (see Parsons 2017).

Finally, designating platforms as regulators generally neglects the role of the state in online regulation. Lawmakers need to clarify platforms' regulatory responsibilities, set appropriate limits, and establish safeguards, not just in regards to hate groups but also in relation to the other social problems that platforms address (see Tusikov 2016). Importantly, academic and policymakers' discussions of platforms' regulatory responsibilities and practices need to account for the vastly different socio-legal environments in which platforms operate. The nature and degree of state involvement will vary by country, reflecting each country's distinctive legal and political frameworks and domestic priorities. Government involvement in internet regulation by authoritarian states will likely differ from that of liberal democratic states. While each may elicit concerns regarding censorship or problematic state surveillance practices, authoritarian states, in particular, often provoke serious concerns of human rights violations. Governments may pressure payment platforms, for example, to disclose user data on political opponents, while law enforcement agencies may seek to use platforms' data to surveil activists, such as Black Lives Matter members.

Conclusion

While we may applaud PayPal and other platforms for terminating their services to hate groups, it is deeply problematic to rely on commercial entities to arbitrate behavior and content considered "acceptable," or to address social problems. Private actors are often perceived as having greater technical skill, specialized access, and the ability to adapt more readily to changing regulatory environments than government regulators are (see Cafaggi 2012). However, platforms' regulatory efforts often have weak due-process mechanisms, lack transparency and accountability measures, and can disproportionately stifle the speech of marginalized populations. Platforms' business interests, moreover, may fundamentally conflict with their regulatory efforts, as their commercial surveillance practices are primarily oriented toward predicting and influencing consumer behavior (Van Dijck 2014; Zuboff 2015), rather than addressing harmful behavior from their users.

Examining how platforms may act as regulators and the consequences of their regulatory practices necessitates a deep understanding of their commercial surveillance activities and the underlying rationales. This article thus brings together two fundamental aspects of platforms: their regulatory capabilities, a private ordering that is reliant on their internal policies, and their surveillance capitalist business models. Large platforms' considerable regulatory capacity has made them attractive as "go to" regulators that are increasingly (informally) tasked to address all manner of social problems. As this article argues, however, platforms' commercial imperatives may trump public regulatory objectives, such as addressing violent hate

groups. Platforms' surveillance capitalist business models operate by collecting and commodifying certain social information as commercially valuable data (datafication) and accumulating and mining data (dataveillance) with the goal of amassing users and predicting future user behavior (Van Dijck 2014; Zuboff 2015). As the Charlottesville and Pittsburgh cases show, certain types of pressure—negative media coverage, political directives, or fear of damage to corporate reputations—can persuade platforms to ban users, even in the absence of formal legal orders.

Recent scholarship on social media platforms examines the negative social implications of platforms' data-intensive business models (e.g., Gillespie 2018; Noble 2018; Vaidhyanathan 2018). However, significant gaps remain in our understanding of other types of platforms, such as those operating as payment or domain name providers. While this article highlights the data-intensive nature of PayPal's business practices, particularly in its acquisition of Venmo, further research in this area is needed. For example, to what extent can surveillance capitalism explain the operation of different types of platforms and how might its expression vary among different socio-legal environments? Further, how do platforms' regulatory activities reflect their distinctive political and legal environments (see e.g., Lv and Luo 2018), and how might different state's internet governance practices affect platforms' commercial and regulatory practices? Research in these areas will help provide a much needed and more nuanced understanding of platforms, their commonalities and variations, and their regulatory and commercial interests.

References

Amend, Alex. 2018. Analysing a Terrorist's Social Media Manifesto: The Pittsburgh Synagogue Shooter's Posts on Gab. *Hatewatch*, Southern Poverty Law Centre, October 28. https://www.splcenter.org/hatewatch/2018/10/28/analyzing-terrorists-social-media-manifesto-pittsburgh-synagogue-shooters-posts-gab [accessed November 14, 2018].

Amend, Alex. 2018a. Silicon Valley's Year in Hate. *Intelligence Report*, Southern Poverty Law Centre, Spring Issue. February 10. https://www.splcenter.org/fighting-hate/intelligence-report/2018/silicon-valleys-year-hate [accessed November 14, 2018].

Belli, Luca and Jamila Venturini. 2016. Private Ordering and the Rise of Terms of Service as Cyberregulation. *Internet Policy Review* 5 (4): 1-17. https://doi.org/10.14763/2016.4.441.

Bond, Shannon. 2018. PayPal's Dan Schulman: Taking on Critics and Dissenters. *Financial Times*, September 9. https://www.ft.com/content/6dc42bbc-af88-11e8-8d14-6f049d06439c [accessed November 20, 2018].

Bridy, Annemarie. 2015. Internet Payment Blockades. *Florida Law Review* 67 (5): 1524-1568.

Cafaggi, Fabrizio, ed. 2012. *Enforcement of Transnational Regulation: Ensuring Compliance in a Global World*. Cheltenham, UK: Edward Elgar Publishing.

CNet. 2018. After Pittsburgh Synagogue Shooting, PayPal Bans Gab Social Network. October 27. https://www.cnet.com/news/after-pittsburgh-synagogue-shooting-paypal-bans-gab-social-network/ [accessed November 22, 2018].

Facebook. 2018. *Community Standards Enforcement Report*. https://transparency.facebook.com/community-standards-enforcement [accessed November 19, 2018].

GAB AI Inc. 2018. *Annual Report*. March 1. https://www.sec.gov/Archives/edgar/data/1709244/000170924418000001/GAB_-_Annual_Report_-_2018.pdf [accessed November 15, 2018].

Gillespie, Tarleton. 2018. *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions that Shape Social Media*. New Haven, CN: Yale University Press.

Glaser, April. 2017. The Internet of Hate. *Slate*, August 30. https://slate.com/technology/2017/08/the-alt-right-wants-to-build-its-own-internet.html [accessed November 11, 2018].

Hankes, Keegan. 2015. PayPal has not Moved to Restrict Hate Groups for Using the Service. *Hatewatch*. Southern Poverty Law Centre, April 1. https://www.splcenter.org/hatewatch/2015/04/01/paypal-has-not-moved-restrict-hate-groups-using-service [accessed November 9, 2018].

Hatewatch Staff. 2017. Organizers and Leaders of Charlottesville's Deadly Rally Raised Money with PayPal. *Hatewatch*, Southern Poverty Law Centre, August 15. https://www.splcenter.org/hatewatch/2017/08/15/organizers-and-leaders-charlottesvilles-deadly-rally-raised-money-paypal [accessed November 10, 2018].

Jan, Tracey. 2017. PayPal Escalates the Tech Industry's War on White Supremacy. *Washington Post*, August 16. https://www.washingtonpost.com/news/wonk/wp/2017/08/16/paypal-escalates-the-tech-industrys-war-on-white-supremacy/?noredirect=on&utm_term=.9f44ff80d0f5 [accessed November 8, 2018].

Klonick, Kate. 2018. The New Governors: The People, Rules, and Processes Governing Online Speech. *Harvard Law Review* 131, no. 6 (April): 1598-1670.

Koren, James Rufus. 2017. Can White Supremacist Groups Be Blocked from Raising Money Online? There's a Campaign to Try. *Los Angeles Times,* August 17. http://www.latimes.com/business/la-fi-alt-right-banking-20170817-story.html [accessed November 11, 2018].

Laidlaw, Emily. 2012. The Responsibilities of Free Speech Regulators: An Analysis of the Internet Watch Foundation. *International Journal of Law and Information Technology* 20: 312-345. https://doi.org/10.1093/ijlit/eas018.

Langenderfer, Jeff. 2009. End-User License Agreements: A New Era of Intellectual Property Control. *Journal of Public Policy & Marketing* 28 (2): 202-211. https://doi.org/10.1509/jppm.28.2.202.

Lee, Timothy B. 2017. Google Explains Why it Banned the App for Gab, a Right-Wing Twitter Rival. *Ars Technica*, August 18. https://arstechnica.com/tech-policy/2017/08/gab-the-right-wing-twitter-rival-just-got-its-app-banned-by-google/ [accessed November 9, 2018].

Lindenbaum, Jeffrey A., and David Ewen. 2012. Catch Me if You Can: An Analysis of New Enforcement Measures and Proposed Legislation to Combat the Sale of Counterfeit Products on the Internet. *Pace Law Review* 32 (3): 567-640.

Lyon, David. 2014. Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique. *Big Data & Society* July-December: 1-13. https://doi.org/10.1177/2053951714541861.

Lv, Aofei, and Ting Luo. 2018. Asymmetrical Power Between Internet Giants and Users in China. *International Journal of Communication* 12: 3878-3895.

Mayer-Schönberger, Viktor, and Kenneth Cukier. 2013. *Big Data: A Revolution that Will Transform How We Live, Work and Think*. London: John Murray.

Mann, Ronald J., and Seth R. Belzley. 2005. The Promise of Internet Intermediary Liability. *William and Mary Law Review* 47: 239-307.

McCoy, Damon, Hitesh Dharmdasani, Christian Kreibich, Geoffrey M. Voelker, and Stefan Savage. 2012. Priceless: The Role of Payments in Abuse-Advertised Goods. *Proceedings of the 2012 ACM Conference on Computer and Communications Security*. New York: ACM. http://dl.acm.org/citation.cfm?id=2382285 [accessed November 14, 2018].

McSherry, Corynne, Jillian C.York, and Cindy Cohn. 2018. *Private Censorship is Not the Best Way to Fight Hate or Defend Democracy: Here are Some Better Ideas*. Electronic Frontier Foundation, January 30.
https://www.eff.org/deeplinks/2018/01/private-censorship-not-best-way-fight-hate-or-defend-democracy-here-are-some

Noble, Safiya Umoja. 2018. *Algorithms of Oppression: How Search Engines Reinforce Racism*. New York: New York University Press.

Paasche, Franz. 2017. PayPal's AUP – Remaining Vigilant on Hate, Violence & Intolerance. *PayPal Stories*. August 15. https://www.paypal.com/stories/us/paypals-aup-remaining-vigilant-on-hate-violence-intolerance [accessed November 4, 2018].

Parsons, Christopher. 2017. The (In)effectiveness of Voluntarily Produced Transparency Reports. *Business & Society* 58 (1): 1-27. https://doi.org/10.1177/0007650317717957.

PayPal. 2015. *Acceptable Use Policy*. Last updated July 1. https://www.paypal.com/ae/webapps/mpp/ua/acceptableuse-full [accessed November 4, 2018].

PayPal. 2018. *PayPal Holdings Inc., Annual Report 2017*. Form 10-K for the United States Securities and Exchange Commission. Filed February 7. http://files.shareholder.com/downloads/AMDA-4BS3R8/6411279711x0xS1633917%2D18%2D29/1633917/filing.pdf [accessed November 4, 2018].

PayPal. 2018a. *User Agreement for PayPal Services*. Last updated November 13. https://www.paypal.com/webapps/mpp/ua/useragreement-full#10 [accessed November 14, 2018].

PayPal. 2018b. *Privacy Policy*, Last updated May 25, https://www.paypal.com/lu/webapps/mpp/ua/privacy-full [accessed November 14, 2018].

PayPal. 2018c. Upholding Our Values: PayPal's Position on Infowars. September 21. https://www.paypal.com/stories/us/upholding-our-values-paypals-position-on-infowars?categoryId=company-news [accessed November 14, 2018].

Schwarcz, Steven L. 2002. Private Ordering. *Northwestern University Law Review* 97 (1): 319-50.

Southern Poverty Law Centre. n.d. https://www.splcenter.org/hate-map [accessed November 1, 2018].

Tenove, Chris, Heidi J.S. Tworek, and, Fenwick McKelvey. 2018. *Poisoning Democracy: How Canada Can Address Harmful Speech Online*. Public Policy Forum, November 8. https://www.ppforum.ca/wp-content/uploads/2018/11/PoisoningDemocracy-PPF-1.pdf [accessed November 10, 2018].

Tusikov, Natasha. 2016. *Chokepoints: Global Private Regulation on the Internet*. Berkeley, CA: University of California Press.

Vaidhynathan, Siva. 2018. *Anti-Social Media: How Facebook Disconnects Us and Undermines Democracy*. Oxford, UK: Oxford University Press.

Van Dijck, José. 2014. Datafication, Dataism and Dataveillance: Big Data between Scientific Paradigm and Ideology. *Surveillance & Society* 12 (2): 197-208. https://doi.org/10.24908/ss.v12i2.4776 .

Venmo. 2018. *Privacy Policy*. Last updated September 19, https://venmo.com/legal/us-privacy-policy/ [accessed November 2, 2018].

Visa. 2018. *Visa Core Rules and Visa Product and Service Rule*s. Last updated October 13, https://usa.visa.com/dam/VCOM/download/about-visa/visa-rules-public.pdf [accessed November 9, 2018].

West, Sarah Myers. 2019. Data Capitalism: Redefining the Logics of Surveillance and Privacy. *Business & Society* 58 (1): 20-41. https://doi.org/10.1177/0007650317718185

Zittrain, Jonathan. 2006. A History of Online Gatekeeping. *Harvard Journal of Law and Technology* 19 (2): 253-298.

Zuboff, Shoshana. 2015. Big Other: Surveillance Capitalism and the Prospects of an Information Civilization. *Journal of Information Technology* 30 (1): 75-89. https://doi.org/10.1057/jit.2015.5.