Tusikov, N. (2021) Censoring Sex: Payment Platforms' Regulation of Sexual Expression. In M. Deflem and DMD Silva, eds. Media and Law: Between Free Speech and Censorship, Volume 26, Series Sociology of Crime, Law and Deviance. (pp. 63-79). Bingley, UK: Emerald Publishing. Page proofs.

CHAPTER 4

CENSORING SEX: PAYMENT PLATFORMS' REGULATION OF SEXUAL EXPRESSION

Natasha Tusikov

ABSTRACT

Purpose – *This chapter examines the role of payment platforms in the United States in sex censorship in which platforms have a pattern of denying financial services to people and businesses involved in publishing legal sexual content. It answers the following questions: what explains payment platforms' regulation of lawful sexual content and what are the consequences?*

Methodology/Approach – *Drawing from the platform governance literature, this chapter closely examines the corporate policies for PayPal and the credit card companies that prohibit certain types of sexual content and services.*

Findings – *This chapter argues that payment platforms' censorship of sexual expression is shaped by the distinctive nature of and market concentration within the online payment industry. Payment actors' systematic campaign of sexual censorship disproportionately affects small businesses and individual operators in the sex and adult entertainment industries and amounts to a form of "digital redlining," a form of financial discrimination.*

Originality/Value – *Payment providers' role in regulating sex online has received considerably less scholarly attention than research on social media platforms. This gap in scholarship is notable as big payment actors have*

Media and Law: Between Free Speech and Censorship
Sociology of Crime, Law and Deviance, Volume 26, 63–79

ISSN: 1521-6136/doi:10.1108/S1521-613620210000026005

systematically denied services for about a decade relating to sexually oriented goods and services (see Blue, 2015a).

Keywords: Payment platforms; sexual expression; censorship; risk; surveillance; financial discrimination

INTRODUCTION

The internet's decade-long "war on sex" has raged across search engines, app stores, social media platforms, and marketplaces with internet platforms banning apps, stores, artistic and educational content, advertising, and products and services related, however tangentially, to sex (see Blue, 2015a). Platforms here refer to two-sided, programable architecture like PayPal that facilitate interactions between businesses and users (van Dijck, Poell, & de Waal, 2018, p. 9). In their anti-sex campaigns, platforms forbid content, product, or services that they variously define as "adult content" (Tumblr, 2020) or "sexually oriented" material (PayPal, 2020a), which often conflates illegal activities, such as communication for prostitution that varies in legality among jurisdictions, and lawful sexual speech. This type of speech is commonly termed adult or "Not Suitable for Work" (NSFW) content that includes videos, photos, artwork, fan fiction, poetry, and music undertaken by a diverse group of people, such as artists, performers, educators, and people working in the sex and adult entertainment industries. This chapter uses the terms adult and sexual content interchangeably.

Online anti-sex campaigns are evident in search engines that downrank search results for adult entertainment websites, app stores that ban apps where users exchange sexual or erotic content, and content delivery networks, which enable the fast delivery of content, banning a social network friendly to sex workers (see Blue, 2015b). Platforms' censorship of sexual speech is typically most visible on large, United States-based social media platforms, particularly Facebook, Instagram, Tumblr, Twitter, and YouTube where content and performers may suddenly vanish. Social media platforms' perception of inappropriate sexual content can extremely broad. Tumblr's definition of adult content, for example, forbids "real-life human genitals or female-presenting nipples" and "any content (including photos, videos, GIFs & illustrations) that depicts sex acts" (Tumblr, 2020), although certain types of artistic, educational, or newsworthy content are generally permitted at the platform's discretion. The platforms' regulation of "obscenity" and inappropriate sexual content particularly focuses on women's bodies, removing content relating to child birth, post-mastectomy scarring, breastfeeding, menstruation, pubic hair, female nipples, as well as banning many types of LGBTQI content (see Chemaly, 2015; Faust, 2017; Roberts, 2019). Critics of social media platforms' sex censorship characterize it as a "kind of cultural genocide on the open internet, one comprised of women, LGBTQI people, artists, educators, bloggers, filmmakers, sex workers, abuse survivors, [and] untold communities" (Blue, 2018).

In contrast to social media platforms, payment providers' role in regulating sex online has received considerably less scholarly attention (a notable exception is Swartz, 2020). This gap in scholarship is notable as big payment actors have systematically denied services for about a decade relating to sexually oriented goods and services (see Blue, 2015a). As journalist, author and activist Violet Blue has documented, banks (such as JP Morgan Chase), credit card associations (namely Visa, Mastercard, and American Express), and payment platforms (like PayPal and Square) have systematically targeted a wide range of people working in the sex trade and retail adult entertainment industry, including escorts, erotic masseuses, adult toy store employees, erotic dancers, cam girls, and performers and models (Blue, 2015a). Payment actors' denial of services for adult content and sexual services makes it difficult for people to get paid via credit or debit cards, bank accounts, or even via crowdfunding sites like Patreon. Proponents of platforms defunding the sex and adult entertainment industries, such as the US National Center on Sexual Exploitation, argue that these industries are inherently exploitative and enable criminal activities like human trafficking, revenge pornography, and child pornography (see McNamara, 2020), a discourse that problematically portrays people working in those industries as victims and lacking agency (see Musto, 2016).

Many of the activities that payment providers target, however, are legal, although the legality of prostitution and escort work varies widely. Even where prostitution is decriminalized, like some Australian states, payment actors continue to deny individuals merchant bank accounts, and, in some cases, personal accounts (see Simpkins, 2019). Australian politician David Limbrick, condemning Australian banks, credit card companies, and platforms for financially discriminating against sex workers and adult retailers, including where prostitution is legal, said their policies "effectively amount to corporate slut shaming" (Simpkins, 2019).

Alongside targeting sex workers and adult industry performers, payment actors also freeze funds or deny their services with regard to sexual expression that does not involve the sale of sexual services. Those in the adult entertainment industry argue that NSFW content is "tech's biggest shadow industry" given its ongoing struggles to secure reliable payment services (Heartpie, 2017). PayPal is particularly active, with Blue characterizing PayPal as "the king of denying service, seizing accounts and freezing funds for anyone discovered to be associated with sexual content online" (Blue, 2015a). Over the past several years, PayPal in the United States has frozen accounts and seized funds relating to the sale of a corset, a memoir written by former escort Vicki Gallas, a sex bloggers' calendar, and submission fees for the Seattle Erotic Art Festival (Blue, 2015a).

Being expelled from social media platforms has the potential to subdue or outright silence targeted individuals, although they may move to other platforms. Payment platforms, however, have the capacity to block payments and suspend accounts temporarily or permanently thereby strangling the ability of individuals or entities to raise donations or sell goods (see Tusikov, 2017, 2019). Losing trusted, commercially popular payment services can destroy businesses, particularly small outfits that do not have the resources or technical capabilities to shift to alternative forms of payment like cryptocurrency (see Andrews, 2019). Payment providers' denial of services with regard to sexually oriented content takes on added significance during the Covid-19 pandemic with the increased vulnerability of already precarious sex workers facing economic downturns and public health restrictions on the types of in-person work they can perform (see DeLacey, 2020).

This chapter examines the role of payment platforms in the United States in sex censorship in which platforms have a pattern of denying financial services to people and businesses involved in publishing legal sexual content. It answers the following questions: what explains payment platforms' regulation of lawful sexual content and what are the consequences? Regulation in this context refers to the process of setting, monitoring, and enforcing rules or standards, whether by state or non-state actors, that involve formal legal or informal mechanisms. The United States is a key site to examine given the global commercial dominance of its internet platforms, including payment providers, and its outsized influence on setting rules and standards relating to how the internet operates and is governed (Tusikov, 2017).

Drawing from the platform governance literature, the chapter closely examines the corporate policies for PayPal and the credit card companies that prohibit certain types of sexual content and services. The chapter argues that payment platforms' censorship of sexual expression is shaped by the distinctive nature of and market concentration within the online payment industry. Despite the growing number of payment methods, there are a handful of dominant payment actors, especially Visa, Mastercard, and PayPal. Further, many payment systems like PayPal, Square, or Apple Pay rely upon the credit card networks, meaning that if the credit card companies forbid a particular activity, that rule also governs the operation of the associated payment provider.

In other words, certain payment actors, particularly the major US credit card companies, exert structural power over the online payment system. They determine the rules and processes for what constitutes acceptable and prohibited transactions and govern who can be granted merchant accounts to accept payments via credit cards. Credit card companies rate most transactions for sexual content and services as high risk, making them pricey to undertake and leaving small merchants with few commercial options. Alongside these market dynamics, 2018 legislation in the United States – the *Fight Online Sex Trafficking Act*, known colloquially as FOSTA/SESTA – is entrenching payment platforms' regulation of sexual speech. The chapter finds that payment actors' systematic campaign of sexual censorship disproportionately affects small businesses and individual operators in the sex and adult entertainment industries and amounts to a form of "digital redlining," a form of financial discrimination.

The chapter proceeds in six parts. First, it explains how payment platforms employ surveillance to govern through data and then explains payment platforms' operation as regulators, including how credit card companies wield power in the online payment ecosystem. Third, the chapter highlights the effect of FOSTA/SESTA on online sexual speech and then argues that the online regulation of sexual speech constitutes digital redlining before providing a brief conclusion.

PLATFORM SURVEILLANCE

Platforms that prioritize the mass accumulation and interpretation of users' personal data as part of their business models operate according to a logic that scholars alternately term platform capitalism (Srnicek, 2017) or surveillance capitalism (Zuboff, 2019). It has become commonplace to note that social media platforms or marketplaces like Amazon employ surveillance-intensive practices with the aim of influencing and predicting consumer behavior through mass, often automated data collection and data analytics to generate revenue and exert market control within industry sectors (see Zuboff, 2019). Platforms are fueled by data, automated and organized by algorithms, and governed through user agreements (van Dijck et al., 2018, p. 9). Payment platforms follow a similar logic (see Martin, 2019; Westermeier, 2020), as is evident by the data-intensive business practices of PayPal and other smaller platforms like Stripe and Square.

Monitoring Bank Customers

While platforms' surveillance-intensive business models are relatively novel, having shifted to data accumulation and monetization in the early 2000s (see Zuboff, 2019), the financial industry in the United States has over a century of experience monitoring their customers. In fact, the roots of contemporary surveillance capitalism within the financial system can be traced back to the beginnings of commercial and consumer credit bureaus, with the latter emerging in the 1870s in the United States following the establishment of commercial credit ratings systems (Lauer, 2018). Josh Lauer's fascinating history of these credit bureaus documents their creation of huge archives of personal information, including the collection of data on customers' marital status, job performance, domestic arrangements, physical appearance, and health, legal and criminal histories (Lauer, 2018). As Lauer (2018, p. 11) argues, corporate credit surveillance facilitated the growth of state surveillance, even assisting the Federal Bureau of Investigation and Internal Revenue Service in the early 1900s given the credit bureaus' vast repositories of personal data.

Surveillance thus is an intrinsic element of the financial system. The early credit bureaus evolved into modern credit giants like Experian that minutely track the spending behavior of over a billion people to determine consumers' financial status and their financial identity in terms of being creditworthy or a credit risk (Lauer, 2018). The credit card companies, which operate as an "invisible surveillance network" (Lauer, 2018, p. 1) pervasively monitors its customers and their transactions, using proprietary algorithms to verify each purchase by checking the customer's spending profile, location, and credit limit and the merchant's location, and either approving the purchase or flagging it as suspicious.

Money is Data

Financial institutions' pervasive surveillance of their individual and corporate customers enables the continued growth of financial transactions and helps manage any risk to their businesses. Historically, financial institutions regarded this data collection as a means to delivering financial services; however, with the increasing incorporation of technology into the financial industry, data collection has taken on an important new dimension. Payment actors traditionally "thrived on money, not data" (Westermeier, 2020, p. 2) but have now adjusted their business models to exploit the economic value of the transactional data they collect. Simply put, "data is the new money, but also, money is data" (Pardes, 2019 cited in Westermeier, 2020, p. 2). More important than the purchase amount is transactional data, including information on the sellers, buyers, shopping histories, payment methods, and customer preferences (Maurer, 2012, p. 477, cited in Westermeier, 2020, p. 2). Data thus becomes an asset. Platforms' aggregation and accumulation of personal data is undertaken to assetize data with the understanding that financial value will be accrued (Birch, Chiappetta, & Artyushina, 2020, p. 11).

Payment platforms' conceptualization of money as data is evident in the granularity of their surveillance of customers' behavior and transactions. PayPal, for example, collects data including, users' mailing and email addresses, telephone numbers, account numbers, shopping history, and geolocation data like IP addresses, as well as users' personal characteristics like national origin, disability, citizenship, and military status (PayPal, 2020b). PayPal also makes inferences based on its collection of personal data with regard to its users' traits, habits, and preferences to personalize users' preferences and to conduct its fraud and risk assessments (see PayPal, 2020b). Platforms' data collection practices and generation of inferential data can raise privacy concerns as transactional data may reveal highly sensitive information about people's political views, religion, health, and sexual habits. By combining different forms of data that until now have been separately collected – and, additionally, not been targeted by payment platforms – enables companies to conduct more comprehensive, personalized assessments of people's social or economic situations (Westermeier, 2020, p. 2).

Payment platforms also collect information not traditionally considered financial data. In 2013, PayPal acquired the Venmo mobile payment application with a social networking function. Designed to let people split payments, Venmo encourages its users to share details with their social networks, posting messages and emojis about their activities and transactions (Venmo, 2020). Unless users' set their Venmo accounts to private, messages about transactions are publicly visible, revealing sometimes sensitive transaction details, such as drug sales where the communication between seller and customers are captioned with emojis describing the purchase and use of marijuana (see Do Thi Duc, 2017). By combining financial data with social media data about their users' contacts, interests, and habits, PayPal can have a granular level of detail about their users that goes far beyond what is traditionally understood as financial credit rating (see Swartz, 2020). Venmo thus has similarities with the Chinese social credit program, designed by the Chinese government and carried out by platforms like Tencent and Alibaba, with the goal of monitoring, controlling, and predicting the trustworthiness – and creditworthiness – of people and companies within the country (Liang, Das, Kostyuk, & Hussain, 2018, p. 415).

PAYMENT PLATFORMS AS REGULATORS

Payment platforms are not new to policing their users for violations of their policies, and can be effective regulators because they have contractual relationships with their users and detailed data on their customers. They have blocked transactions and terminated accounts with regard to a range of illegal or unwanted activities, including copyright infringement (Bridy, 2015), child pornography (Laidlaw, 2015), counterfeit goods (Tusikov, 2017), hate speech (Tusikov, 2019), and sexually explicit content and services (Swartz, 2020).

Created in 1998, PayPal is an online payment company that performs money transfers and processes payments. In 2019, PayPal had 305 million active accounts and facilitated US$12.4 billion payment transactions with a total payment volume of US$712 billion, while Venmo processed over $102 billion in 2019 (PayPal, 2020c). PayPal's policies prohibit transactions involving "items that are considered obscene" and "certain sexually oriented materials or services" (PayPal, 2020a, 2(g), 2(i)). PayPal may also terminate its services to merchants if their transactions post any "legal, reputational, or risk-based reason" (PayPal, 2020d, Section 9.2(3-4)). If the company determines that its seller's "transactions pose an unacceptable level of risk," the platform may refuse to process transactions, hold payments, or limit or suspend the seller's ability to use the payment services (PayPal, 2020d, Section 5.2). Like most platforms, the company reserves the right to suspend or terminate access to any of its services "for any reason and at any time upon notice to you" (PayPal, 2020e).

Online Payment Ecosystem

Given the number of actors potentially involved in a transaction, it can be difficult to determine which actor ordered a transaction to be blocked or account closed. Payment actors tend to blame each other when the disputes become public (see Malcolm, 2017), underscoring the complexity of the payment ecosystem and the opacity which enables actors to shift blame to others.

There are a wide variety of digital payment methods for merchants to accept payments, ranging from services by big US technology firms like Apple Pay and Google Pay to smaller firms like WePay, Stripe, Square, and the Dutch platform Adyen. Despite this diversity, many payment platforms rely upon the traditional brick-and-mortar banks to grant merchant bank accounts and the credit card system to enable customers to pay with credit cards. PayPal's services rely upon the existing credit card networks, as well as the automated clearinghouse, a utility partially operated by the US Federal Reserve, that enables customers to link their PayPal account directly to their checking account to transfer funds, thereby creating “a private on-ramp to an existing semi-public infrastructure” (Swartz, 2020, p. 39).

As banks and the credit card system provide this vital, largely invisible infrastructure, they set the rules governing the use of their services. Visa and Mastercard are particularly powerful in this regard given their global duopoly on the credit card market outside China, with Visa controlling 60 percent of the credit and debit card market and Mastercard at 30 percent, while American Express trails far behind at about 8 percent (Krauskopf, 2020). Given their dominance, when Visa and Mastercard prohibit transactions relating to specific products or services, all payment providers using their credit card network must abide by the credit card network’s rules.

Payment providers design their services to make the transfer of funds rapid and easy. Behind the simple interface, however, there is an often–complex network of contractual obligations and rules with multiple actors depending on the payment type. Stripe describes this as living “in a tangled thicket of regulations and restrictions” (Lyon, 2016). To transfer funds between bank accounts, for example, PayPal and Square must abide by rules set by banks. To facilitate payments via credit card, the platforms must obey rules set by credit card networks (e.g., Visa, Mastercard, and American Express), as must the banks that granted the credit card to cardholders (issuing institutions) and the banks that granted the merchant account that accepts credit card payments (acquiring institutions). Square, for example, in the United States offers payment through credit cards operated by the banks JPMorgan Chase and Wells Fargo. As a result, merchants using PayPal or Square must comply with the rules of the platforms, the credit card networks, and acquiring institutions.

As the card networks do not have direct contractual relationships with merchants, they cannot restrict or terminate access to merchant accounts since affiliated banks granted them. Instead, the card networks instruct acquiring institutions like Wells Fargo to investigate suspicious behavior and take appropriate action, which includes the termination of merchant accounts.

American Express has a blanket prohibition on transactions relating to escort services, massage parlors, online adult entertainment, and prostitution (American Express, 2020). Visa and Mastercard permit transactions regarding certain types of adult content and services, provided the transaction is legal in both the buyer’s and sellers’ jurisdictions. They also grant themselves latitude to interpret the suitability of merchants’ products and services with regard to how it may affect their brands, prohibiting any transactions that may bring their brands “into disrepute” (Visa, 2020, p. 79). Mastercard’s policies are more detailed than Visa’s, prohibiting “the sale of a product or service, including an image, which is patently offensive and lacks serious artistic value” and gives as examples of “offensive” non-consensual sexual behavior, sexual exploitation of a minor, or “or any other material” the company deems “unacceptable” (Mastercard, 2019, p. 109).

The credit card networks have interpretive flexibility given their broadly worded policies to determine, in Mastercard’s terms, what counts as “offensive,” "unacceptable," and "serious artistic value," thereby leading to sometimes arbitrary determinations of acceptable transactions. In 2017, for example, Visa and Mastercard withdrew their services from the adult social network FetLife, which describes itself as "Facebook but run by kinksters," because, it appears, that the platform offered members a forum to discuss and post-depictions of consensual BDSM practices (Malcolm, 2017). While it appears that the credit card AQ1 companies ordered the termination of FetLife's payment services, neither Visa nor Mastercard prohibit transactions relating to consensual BDSM. As of July 2020, FetLife still does not accept payment through credit cards.

As the FetLife case shows, given the lack of transparency and clarity around the credit card companies' rules and decisions, it is not always evident why a specific product or type of content might be banned other than a generic explanation that it is "high risk" or "unacceptable." The payment provider Stripe criticizes blanket prohibitions against certain types of legal content and services, stating that rather than evaluating businesses individually, "many financial institutions choose to make decisions around broad categories of business" in which "restrictions can function more like hammers than scalpels" (Lyon, 2016).

Fines are a key mechanism by which the credit card networks ensure compliance with its rules. PayPal, for example, explains that it is subject to the network's fines if the platform fails to detect merchants "engaging in activities that are illegal or considered 'high risk'" (PayPal, 2020f, p 13). PayPal can either prevent high-risk merchants from using its services or register them with the card networks and "conduct additional monitoring" as required (PayPal, 2020f, p 13).

Banned Merchants Database

A key part of the financial ecosystem that affects the regulation of adult content is a proprietary database used by credit card companies that lists terminated merchants, the "MATCH" list (the Member Alert to Control High Risk Compliance Program) (see Mastercard, 2020). This global database, developed and maintained by Mastercard and accessible to American Express, lists merchants worldwide who have violated the credit card companies' rules. Visa has its own Terminated Merchant List database. Credit card companies typically require acquiring institutions to check the databases before granting applicants merchant accounts to see if merchants have had their merchant accounts terminated by another acquirer and the reasons given.

Acquirers may terminate merchant accounts for specific violations, termed "reason codes," that include illegal transactions, violation of standards like engaging in prohibited transactions, and excessive chargebacks (Mastercard, 2020, pp. 123–124). Once terminated for a specific reason code, acquiring institutions must add terminated merchants to MATCH. Terminated merchants are often considered to be a higher risk and less likely to be granted new merchant accounts by other acquiring institutions. Even if an individual has been terminated, another financial institution can decide to grant a merchant account provided the institution requires the merchant to implement certain changes, such as instituting anti-fraud measures.

Problematically, Mastercard does not verify or confirm the accuracy of the information contained in the MATCH system as it relies upon submissions from acquiring institutions (Mastercard, 2020). Blacklisted merchants can only be removed from the database if the information was incorrect, or the acquiring institution verifies that the merchant addressed the underlying problem. Only the submitting acquiring institution can remove faulty information, meaning that inaccurate information persists until removal or until the five-year limit is reached and all information is deleted.

The credit card companies thus play major roles in creating and maintaining the financial infrastructure upon which much of the digital payment system operates. Visa, Mastercard, and American Express set the rules governing the use of their services, which their networks of affiliated financial institutions must obey if they want to offer their credit cards. The power of rule setting is particularly evident with regard to the MATCH database where acquiring institutions globally assess and terminate merchants in accordance with criteria and processes set by Mastercard. Visa and Mastercard, given their dominant market share, can effectively establish payment "chokepoints" where blacklisted entities often have few other payment options (Tusikov, 2017).

"Being Mainstream Is Cheap"

"Being mainstream is cheap while being NSFW is risky," explains Heartpie, a California-based social network where users can purchase individual subscriptions for or crowdsource the creation of original, custom-tailored adult content (Heartpie, 2017). Sexual content and services, along with other issues like gambling, are considered high risk because of the perceived likelihood of fraud or chargebacks, which expose companies to higher costs and potential liability. Chargebacks are a form of disputed transaction in which the customer asks the card issuer to reverse the transaction.

The payment ecosystem becomes more complicated for smaller players like Heartpie that want to accept credit card payments. Large merchants like department stores connect directly to acquiring banks, but small merchants have their credit card payments paid through an independent sales organization (ISO) that acts as an intermediary between merchants and acquiring institutions (Swartz, 2020). Payment actors sort merchants into risk categories with those having similar probability of chargebacks priced similarly, and some ISOs specialize in high-risk payments for which they charge merchants higher fees (Swartz, 2020, p. 87). As a result, people selling sexually oriented goods and services typically must pay higher payment processing fees.

Sexual speech is caught in the clash between what Swartz (2020, p. 91) describes as the "traditional" and "platform" models of payment that has significantly changed the management of risk. In the traditional model, cardholders' interests are represented by issuing institutions, while merchants' interests are represented by acquiring institutions (Swartz, 2020, p. 91). There is a market for risk as high-risk transactions create market categories for pricing (Swartz, 2020, p. 96). High-risk transactions aren't banned, they are pricy for merchants.

In contrast, in the platform model, neither buyers nor sellers are directly represented as the client is the platform like PayPal (Swartz, 2020). Unlike traditional ISOs that have customizable contracts with their merchants to accommodate all levels of risk, payment platforms govern their users with blanket terms-of-service contract. Risk is not managed through the market, but banned in terms-of-service agreements (Swartz, 2020, p. 93). High-risk transactions are typically banned because payment platforms like PayPal must guarantee that all their transactions will be low risk for chargeback to qualify for the lowest rates (Swartz, 2020, p. 93).

An entity that can offer a certain scale of transactions like Heartpie can seek out "special adult-friendly payment processors who have an arrangement with their bank to provide merchant accounts to high-risk merchants" (Heartpie, 2017). Adult content merchants can still process payments, but they generally lack access to mainstream providers and low-risk transaction pricing. Individuals and small-scale businesses, however, have few options as neither the traditional nor platform models cater to "high-risk" categories of person-to-person transactions (Swartz, 2020, p. 94).

LAWS ENTRENCHING FINANCIAL DISCRIMINATION

Payment providers' anti-sex stance in the United States has become more entrenched in 2018 with the passage of the *Fight Online Sex Trafficking Act* (FOSTA) and the *Stop Enabling Sex Traffickers Act* (SESTA). Signed into law in April 2018, SESTA, which was effectively subsumed into FOSTA, controversially expand US federal prostitution laws by making internet platforms legally responsible for third-party content that promote or facilitate prostitution with imprisonment of up to 10 years for platform operators. Prior to FOSTA/SESTA, Section 230 of the 1996 *Communications Decency Act*, referred to as the "safe harbor" law, and one of the most important pieces of legislation that built the internet, granted broad immunity to platforms for some types of speech by users, including sexual expression. These laws rolled back part of this immunity, meaning entities providing web hosting, social media, search, or payment services could be liable for their users' content, even for legal forms of sex work.

Legislators and advocates justified FOSTA/SESTA as necessary to combat human trafficking but, as a mounting body of research demonstrates, the laws have not reduced trafficking but made sex work more dangerous by eliminating protections (Chamberlain, 2019). As critics of the law note, the combination of the laws' overbroad language, strict penalties, and repeal of platform's previous immunity for content posted by their users mean that platforms will categorically ban entire categories of sexual expression (Chamberlain, 2019, p. 2197).[1]

DIGITAL REDLINING

Platforms' anti-sex campaign can be understood as a form of "digital redlining," a continuation of the discriminatory financial practice of redlining that was legal in the United States from the early 1930s to the late 1960s when it was prohibited. Redlining was a set of policies designed to suppress homeownership by Black people: banks denied mortgages, governments funneled money to white homeowners, and communities created "whites-only" subdivisions using zoning laws and predatory contracts (Friedline & Chen, 2020). Discriminatory financial practices continue in the United States with banks targeting racialized, largely Black communities for risky subprime mortgages, who also pay a disproportionate local tax burden (see Van Dam, 2020).

Digital redlining has been used to explain platforms' discriminatory advertisements practices that enable real estate brokers and landlords to exclude certain buyers or renters from seeing ads (Karlis, 2019), and the predatory targeting of low-income and minority communities for harmful or inferior products like for-profit education (Gilman, 2019). In finance, digital redlining occurs at the nexus of finance and digital technologies, involves multiple reinforcing policies, and creates differential, discriminatory access to financial services, in part because of the digital divide in broadband internet access, with racialized communities disproportionately affected (Friedline & Chen, 2020).

Digital redlining with regard to sexual speech is the part of a systematic, multifaceted campaign undertaken by multiple actors within the online payment ecosystem that disproportionately affects small businesses and individual operators in the sex and adult entertainment industries (see Blue, 2015a). Regulatory efforts often appear arbitrary, as shown by PayPal's bans of sales relating to escorts' memoirs or corsets discussed in the introduction. However, a common element of many of the media-reported cases of sexual censorship is the targeting of small businesses and individuals, but facilitating business for larger companies. Visa and Mastercard have permitted transactions for pornography businesses, as anti-pornography campaigns against the credit card companies demonstrate (Mohan, 2020). Even sex-adverse American Express is trialing a program allowing users in the United States to pay for a pornography-streaming service (Mohan, 2020).

Companies within the sex and adult entertainment industries, typically larger players that have a certain scale of transactions, may be able to negotiate a contract with an ISO specializing in high-risk transactions or guarantee a low rate of chargebacks. Simply put, bigger actors can better manage risk and afford fees, while smaller operators have few options (see Swartz, 2020). This may explain PayPal's 2019 termination of its services to Pornhub's Model Program, which allows performers to upload and an earn revenue from videos they create themselves (see Cole, 2019).[2] Pornhub itself is big business, as the largest free, ad-supported adult-video streaming service with 120 million visitors daily, and it makes it money from paid membership subscriptions and advertising. However, its Model Program's performers seemingly operate like contractors and earn revenue independently through Pornhub by selling videos and advertising revenue, and, as individuals, have no collective way to negotiate with an ISO specializing in high-risk transactions.

Payment actors' systemic financial discrimination against sex workers is evident even where sex work is decriminalized, such as in the Australian states of Victoria and New South Wales. Australia's Small Business and Family Enterprise Ombudsman, Kate Carnell, accuses financial institutions in Australia of wrongly discriminating against legitimate small businesses in the adult sector, which is estimated at 25,000 people with an annual turnover of AUS$2.6 billion (Simpkins, 2019). Despite the overall size of the sector, its small businesses and individual operators struggle to receive merchant accounts with platforms like PayPal, Square, and Stripe banning or restricting their services related to the sale of sexual services (Sex Work Law Reform Victoria, 2020). As advocacy groups point out, payment actors perceive risk in differing legal approaches to sex work among Australian states: a nationwide decriminalization of sex work could ensure equitable access financial services (see Sex Work Law Reform Victoria, 2020).

FOSTA/SESTA have intensified payment platforms' anti-sex measures as the laws have increased platforms' risk of allowing any content or transactions that may be perceived to promote or facilitate prostitution. The chilling effect predicted by the law's critics is occurring, not only in the United States but also internationally. A 2019 survey undertaken by a US collective of sex workers and allies of 98 internet-based sex workers, mostly in the United States, but also some in Canada, Europe, Australia, and South America found sex workers reported less ability to advertise their services, vet clients, and control their working environments (Blunt & Wolf, 2020). In Vancouver, the PACE Society, AQ2 which provides sex worker-led programs, finds many United States-based websites have shut down, and without the ability to advertise and digitally screen clients, Canadian sex workers are forced to operate in unsafe conditions (Tierney, 2018).[3]

CONCLUSION

The internet war on sex rages globally with many countries seeking to suppress various forms of sexual speech, but it has distinct roots in the United States given the commercial dominance of US platforms and the role of the United States in shaping rules and standards on the internet that are instituted worldwide (see Tusikov, 2017). Simply put, US norms and rules become universalized into global rules through large US companies and their global networks. As new digital payment methods like Apple Pay, PayPal, or Square are often built upon the existing banking and credit card infrastructure, over which the United States exerts structural power, banks, and credit card companies act as gatekeepers. Visa and Mastercard wield particular structural power given their dominant market share. When Visa and Mastercard forbid certain types of transactions, the prohibitions reverberate throughout the online payment industry with their networks of banks and payment providers required to institute their rules or face stiff fines. While Visa and Mastercard allow some sexual content, including legal pornography, this permission is contingent upon the credit card networks' interpretation that the transactions are not bringing the companies' brands "into disrepute" (Visa, 2020, p. 79).

This is the essence of payment actors' structural power. People in smaller countries like Canada, Australia, or Mexico which use US platforms and businesses find they must also accept US rules, even when they may conflict with national or local laws.

In the traditional payment model, credit card companies surveilled consumers to manage risk in order to facilitate transactions (see Lauer, 2018), the platform payment model focuses not only on risk management but also consumer surveillance as part of its business model (Swartz, 2020, see also Westermeier, 2020). Platforms' data-intensive business model enables them not only to discern patterns in users' behavior for the development of future products and services, but also to sort users into risk categories based on their sales of sexual content and services. In some cases, platforms have shifted their focus from targeting adult content as a "high-risk *transaction*," to designating those in the sex industry as "high-risk *people*" (Swartz, 2020, p. 97, emphasis in original). PayPal did this in 2010 when it banned dominatrix January Seraph in 2010 and any business run or owned by her "for life" (Blue, 2015a), a grossly disproportionate and discriminatory penalty that bluntly targets a person not a specific prohibited activity. Payment platforms' mass accumulation of data from different sources, including social media, means that they have a capacity to make inferences about people's economic circumstances and their social activities and a largely opaque and unaccountable power to designate people as high risk.

This chapter highlights the role of dominant US actors in setting rules regarding permitted sexual content, but significant gaps remain in our understanding of payment platforms' regulation of online sexual speech. More empirical research is needed regarding the scope and nature of payment actors' restrictions on sexual expression, particularly among smaller and non-US payment platforms. What political, regulatory, and socio-cultural factors figure into non-US payment platforms' regulation of sexual content? To what extent might there be differing legal or socio-cultural interpretations of permitted and prohibited sexual speech among payment actors, and with what consequences? Cindy Gallop, founder of the female-focussed pornography platform Make Love Not Porn, argues that laws and platforms' terms-of-conditions agreements "were written for porn," meaning that there is a "need for a new legal definition of adult content" with regards to "sextech and sex education" (Deighton, 2020). Analysis determining the legal, regulatory, or material incentives that might encourage payment actors to adopt more nuanced definition of adult content could be a useful first step to address the problems of digital redlining and the financial exclusion of those in the sex and adult entertainment industries.

NOTES

1. Problematically, FOSTA and SESTA conflate consensual sex work with sex trafficking, a common practice strategically employed by opponents of the sex industry, some of whom are prominent civil society organizations with the goal of outlawing all sex work (see Musto, 2016).
2. Pornhub is a controversial site with critics contending that it does not effectively remove revenge porn, which is the non-consensual uploading of porn, or content relating to rape and sexual abuse (Cole & Maiberg, 2020).

3. For a list of websites and online services shut down because of SESTA/FOSTA, see: https://survivorsagainstsesta.org/documentation/

REFERENCES

American Express. (2020, July). Merchant operating guide. United States, including Puerto Rico and the US Virgin Islands. Retrieved from https://icm.aexp-static.com/content/dam/gms/en_us/optblue/us-mog.pdf. Accessed on July 18, 2020.

Andrews, I. (2019, October 30). Cryptocurrency for sex workers and their clients. *Medium*. Retrieved from https://medium.com/@lafemmeisobel/cryptocurrency-for-sex-workers-and-their-clients-bee59466eb46. Accessed on July 11, 2020.

Birch, K., Chiappetta, M., & Artyushina, A. (2020). The problem of innovation in technoscientific capitalism: Data rentiership and the policy implications of turning personal digital data into a private asset. *Policy Studies*. AQ3

Blue, V. (2015a, December 2). PayPal, Square and big banking's war on the sex industry. *Engadget*. Retrieved from https://www.engadget.com/2015-12-02-paypal-square-and-big-bankings-war-on-the-sex-industry.html. Accessed on July 23, 2020.

Blue, V. (2015b, February 24). Timeline: Google's role in global sex censorship. *ZDNet*. Retrieved from https://www.zdnet.com/article/timeline-googles-role-in-global-sex-censorship/. Accessed on July 22, 2020.

Blue, V. (2018, December 7). The internet war on sex is here. *Engadget*. Retrieved from https://www.engadget.com/2018-12-07-the-internet-war-on-sex-is-here.html. Accessed on July 20, 2020.

Blunt, D., & Wolf, A. (2020). Erased: The impact of FOSTA–SESTA and the removal of Backpage on sex workers. *Anti-Trafficking Review*, *14*, 117–121.

Bridy, A. (2015). Internet payment blockades. *Florida Law Review*, *67*(5), 1523–1568.

Chamberlain, L. (2019). FOSTA: A hostile law with a human cost. *Fordham Law Review*, *87*, 2171–2211.

Chemaly, S. (2015). Slut-shaming and the sex police: Social media, sex, and free speech. In S. Tarrant (Ed.), *Gender, sex and politics: In the streets and between the sheets in the 21st century* (pp. 125–140). New York, NY: Routledge.

Cole, S. (2019, November 14). PayPal pulls out of Pornhub, hurting 'hundreds of thousands' of performers. *Vice*. Retrieved from https://www.vice.com/en_ca/article/d3abgv/paypal-pulls-out-of-pornhub-payments. Accessed on July 3, 2020.

Cole, S., & Maiberg, E. (2020, February 6). Pornhub doesn't care. *Vice*. Retrieved from https://www.vice.com/en_us/article/9393zp/how-pornhub-moderation-works-girls-do-porn. Accessed on August 3, 2020.

Deighton, K. (2020, May 10). Why sex startups face uphill payments battle. *Raconteur*. Retrieved from https://www.raconteur.net/finance/sextech-payments. Accessed on July 11, 2020.

DeLacey, H. (2020, May 10). The precaritisation of sex worker during the COVID-19 pandemic. *Leiden Law Blog*. Retrieved from https://leidenlawblog.nl/articles/the-precarisation-of-sex-workers-during-the-covid-19-pandemic. Accessed on July 16, 2020.

Do Thi Duc, H. (2017). Public by default. Retrieved from https://22-8miles.com/public-by-default/. Accessed on July 25, 2020.

Faust, G. (2017). Hair, blood and the nipple. In U. Undine Frömming, S. Köhn, S. Fox, & M. Terry (Eds.), *Digital environments: Ethnographic perspectives across global online and offline spaces* (pp. 159–170). Bielefeld: Transcript-Verlag.

Friedline, T., & Chen, Z. (2020). Digital redlining and the Fintech marketplace: Evidence from US zip codes. *The Journal of Consumer Affairs*.

Gilman, S. (2019). Proliferating predation: Reverse redlining, the digital proliferation of inferior social welfare products, and how to stop it. Retrieved from https://ssrn.com/abstract=3511892. Accessed on July 10, 2020.

Heartpie. (2017, May 8). nsfw's payment processing problem. *Medium*. Retrieved from https://medium.heartpie.com/nsfws-payment-processing-problem-aa0d53c0ea2f. Accessed on July 8, 2020.

Karlis, N. (2019, August 21). "Digital redlining:" Faceook's housing ads seem designed to discriminate. *Salon*. Retrieved from https://www.salon.com/2019/08/21/digital-redlining-facebooks-housing-ads-seem-designed-to-discriminate/. Accessed on July 17, 2020.

Krauskopf, L. (2020, January 31). Swiping their way higher: Visa, Mastercard could be the next $1 trillion companies. *Reuters*. Retrieved from https://www.reuters.com/article/us-visa-Mastercard-stocks/swiping-their-way-higher-visa-Mastercard-could-be-the-next-1-trillion-companies-idUSKBN1ZU0JA. Accessed on July 10, 2020.

Laidlaw, E. (2015). *Regulating speech in cyberspace: Gatekeepers, human rights and corporate responsibility*. Cambridge: Cambridge University Press.

Lauer, J. (2018). *Creditworthy: A history of consumer surveillance and financial identity in America*. New York, NY: Columbia University Press.

Liang, F., Das, V., Kostyuk, N., & Hussain, M. M. (2018). Constructing a data-driven society: China's social credit system as a state surveillance infrastructure. *Policy & Internet*, *10*(4), 415–453.

Lyon, D. (2016, August 12). Why some businesses aren't allowed. *Strip Blog*. Retrieved from https://stripe.com/blog/why-some-businesses-arent-allowed. Accessed on July 12, 2020.

Malcolm, J. (2017, March 15). Payment processors are still policing your sex life, and the latest victim is FetLife. *Electronic Frontier Foundation*. Retrieved from https://www.eff.org/deeplinks/2017/03/payment-processors-are-still-policing-your-sex-life. Accessed on July 2, 2020.

Martin, A. (2019). Mobile money platform surveillance. *Surveillance & Society*, *17*(1/2), 213–222.

Mastercard. (2019). Mastercard rules. Last updated December 19. Retrieved from https://www.Mastercard.us/content/dam/mccom/global/documents/Mastercard-rules.pdf. Accessed on July 18, 2020.

Mastercard. (2020, February 27). Security rules and procedures. *Merchant Edition*. Retrieved from https://www.merchantmaverick.com/learning-terminated-merchant-file-tmf-aka-match-list/. Accessed on July 27, 2020.

McNamara, H. (2020, February 24). Credit card companies should stop partnering with porn websites. *Washington Examiner*. Retrieved from https://www.washingtonexaminer.com/opinion/op-eds/credit-card-companies-should-stop-partnering-with-porn-websites. Accessed on July 27, 2020.

Mohan, M. (2020, May 8). Call for credit card freeze on porn sites. *BBC*. Retrieved from https://www.bbc.com/news/world-52543508. Accessed on August 5, 2020.

Musto, J. (2016). *Control and protect: Collaboration, carceral protection, and domestic sex trafficking in the United States*. Oakland, CA: University Press.

PayPal. (2020a). Acceptable use policy. Last updated March 19. Retrieved from https://www.paypal.com/us/webapps/mpp/ua/acceptableuse-full?locale.x=en_US. Accessed on July 19, 2020.

PayPal. (2020b). Privacy statement. Effective May 13. Retrieved from https://www.paypal.com/us/webapps/mpp/ua/privacy-full?locale.x=en_US. Accessed on July 11, 2020.

PayPal. (2020c, January 29). PayPal reports fourth quarter and full year 2019 results. Retrieved from https://www.paypal.com/stories/us/paypal-reports-fourth-quarter-and-full-year-2019-results. Accessed on July 27, 2020.

PayPal. (2020d). Platform Seller Account Agreement, Section 9.2(3 and 4). Last updated April 2. Retrieved from https://www.paypal.com/us/webapps/mpp/ua/platform-seller-agreement?locale.x=en_US. Accessed on July 19, 2020.

PayPal. (2020e). User agreement. Effective as of April 28. Retrieved from https://www.paypal.com/us/webapps/mpp/ua/useragreement-full?locale.x=en_US. Accessed on July 19, 2020.

PayPal. (2020f, April 8). 2020 Annual Meeting of Stockholders and Proxy Statement & 2019 Annual Report. Retrieved from https://investor.paypal-corp.com/static-files/6b4a31d7-9941-464d-846d-3859fd7058dc. Accessed on July 28, 2020.

Roberts, S. (2019). *Behind the screen: Content moderation in the shadows of social media*. New Haven, CT: Yale University Press.

Sex Work Law Reform Victoria. (2020). Financial institutions: Which ones discriminate? Retrieved from https://sexworklawreformvictoria.org.au/financial-institutions-which-ones-discriminate/. Accessed on August 1, 2020.

Simpkins, S. (2019, November 18). Sex worker blasts fintechs for discrimination. *Fintech Business*. Retrieved from https://www.fintechbusiness.com/payments/1586-sex-worker-blasts-fintechs-for-discrimination. Accessed July 19, 2020.

Srnicek, N. (2017). *Platform capitalism*. Cambridge: Polity Press.

Swartz, L. (2020). *New money: How payment became social media*. New Haven, CT: Yale University Press.

Tierney, A. (2018, April 12). How the US 'sex trafficking' crackdown is hurting sex workers in Canada. *Vice*. Retrieved from https://www.vice.com/en_ca/article/9kggwe/how-the-us-sex-trafficking-crackdown-is-hurting-sex-workers-in-canada. Accessed on August 5, 2020.

Tumblr. (2020). Community guidelines. Last modified July 16. Retrieved from https://www.tumblr.com/policy/en/community. Accessed on July 17, 2020.

Tusikov, N. (2017). *Chokepoints: Global private regulation of the internet*. Oakland, CA: University of California Press.

Tusikov, N. (2019). Defunding hate: PayPal's regulation of hate groups. *Surveillance & Society*, *17*(1/2), 46–53. https://doi.org/10.24908/ss.v17i1/2.12908

Van Dam, A. (2020, July 2). Black families pay significantly higher property taxes than white families, new analysis shows. *Washington Examiner*. Retrieved from https://www.washingtonpost.com/business/2020/07/02/black-property-tax/. Accessed on July 22, 2020.

van Dijck, J., Poell, T., & de Waal, M. (2018). *The platform society: Public values in a connective world*. New York, NY: Oxford University Press.

Venmo. (2020). Privacy policy. Last updated June 30. Retrieved from https://venmo.com/legal/us-privacy-policy/. Accessed on July 10, 2020.

Visa. (2020, April 18). Visa core rules and visa product and service rules. Version 1.1. Retrieved from https://usa.visa.com/support/consumer/visa-rules.html. Accessed on July 27, 2020.

Westermeier, C. (2020). Money is data: The platformization of financial transactions. *Information, Communication & Society*.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the New Frontier of Power*. New York, NY: Public Affairs.

LEGISLATION

Allow States and Victims to Fight Online Sex Trafficking Act, 1H.R. 1865, 115th Congress. Retrieved from https://www.govtrack.us/congress/bills/115/hr1865/text

Communications Decency Act. S. 314. 47 USC. § 230, 104th Congress (1995–1996). Retrieved from https://www.congress.gov/bill/104th-congress/senate-bill/314/

Stop Enabling Sex Traffickers Act of 2017, S.1693, 115th Congress (2017–2018). Retrieved from https://www.congress.gov/bill/115th-congress/senate-bill/1693

AUTHOR QUERIES

AQ1: Please expand BDSM at first mention in the text.
AQ2: Please expand PACE here.
AQ3: Please provide the volume number and page number for the references: Birch et al. (2020); Friedline & Chen (2020); Westermeier (2020).